Notes

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

⚠️ **CAUTION:** A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

---

**Information in this publication is subject to change without notice.**

Copyright © 2018 Dell EMC Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell EMC® and the Dell EMC logo are trademarks of Dell EMC Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.


2018 - June   Rev. A04
Contents

1 Dell EMC Networking CLI ................. 97
   Introduction .................................. 97
   Command Groups ................................ 98
   Mode Types .................................. 103

2 Using the CLI ............................... 223
   Introduction .................................. 223
   Entering and Editing CLI Commands .......... 223
   CLI Command Modes ......................... 237
   Starting the CLI ............................... 251
   Using CLI Functions and Tools .............. 252

3 Layer 2 Switching Commands .......... 265
   ACL Commands ................................ 266
      ACL Logging ................................ 266
      Commands in this Section .................. 269
      ip access-list ............................... 269
      deny | permit (IP ACL) ...................... 270
deny | permit (Mac-Access-List-Configuration)
ip access-group

. .

276

. . . . . . . . . . . . . . . . . .

279

mac access-group

. . . . . . . . . . . . . . . . .

mac access-list extended

. . . . . . . . . . . . .

mac access-list extended rename .
remark

281
283

. . . . . . . .

283

. . . . . . . . . . . . . . . . . . . . . . .

284

service-acl input

. . . . . . . . . . . . . . . . . .

286

show service-acl interface .

. . . . . . . . . . . .

287

show access-lists interface

. . . . . . . . . . . .

288

. . . . . . . . . . . . . . . .

288

show ip access-lists

show mac access-lists .

. . . . . . . . . . . . . .

292

MAC Address Table Commands . . . . . . . . . . . . . . . .294
Commands in this Section
clear mac address-table

. . . . . . . . . . . . .

295

. . . . . . . . . . . . . .

295

mac address-table aging-time

. . . . . . . . . . .

296

mac address-table multicast forbidden
address

. . . . . . . . . . . . . . . . . . . . . . .

mac address-table static .

. . . . . . . . . . . . .

switchport port-security (Global Configuration)

297
298

. .

299

. . . . . . . . . . . . . . . . . . .

302

switchport port-security (Interface
Configuration) .

Contents

6


show mac address-table multicast ................. 307
show mac address-table ............................. 308
show mac address-table address .................. 309
show mac address-table count ...................... 310
show mac address-table dynamic .................. 311
show mac address-table interface .................. 312
show mac address-table static ..................... 313
show mac address-table vlan ....................... 314
show port-security .................................. 315

**Auto-VoIP Commands** .......................... 318

Commands in this Section ......................... 318
show switchport voice .............................. 319
switchport voice detect auto ...................... 321

**CDP Interoperability Commands** ............... 322

Commands in this Section ......................... 322
clear isdp counters ................................ 322
clear isdp table ..................................... 323
isdp advertise-v2 ................................... 323
isdp enable .......................................... 324
isdp holdtime ....................................... 325
isdp timer ............................................ 326
show isdp ............................................ 326
show isdp entry ........................................ 327
show isdp interface .................................. 328
show isdp neighbors .................................. 329
show isdp traffic ...................................... 330

**DHCP Layer 2 Relay Commands .................. 332**

- Commands in this Section .......................... 332
- dhcp l2relay (Global Configuration) .......... 333
- dhcp l2relay (Interface Configuration) ...... 333
- dhcp l2relay circuit-id ............................... 334
- dhcp l2relay remote-id ............................... 335
- dhcp l2relay trust ................................... 335
- dhcp l2relay vlan .................................... 336
- show dhcp l2relay all ............................... 337
- show dhcp l2relay interface ....................... 338
- show dhcp l2relay stats interface ............... 338
- show dhcp l2relay agent-option vlan .......... 339
- show dhcp l2relay vlan .............................. 340
- show dhcp l2relay circuit-id vlan ............... 341
- show dhcp l2relay remote-id vlan ............... 342
- clear dhcp l2relay statistics interface ........ 342

**DHCP Snooping Commands ....................... 344**

- Commands in this Section .......................... 345
clear ip dhcp snooping binding .......................... 345
clear ip dhcp snooping statistics ......................... 346
ip dhcp snooping ........................................ 346
ip dhcp snooping binding .............................. 347
ip dhcp snooping database ............................ 348
ip dhcp snooping database write-delay ............... 349
ip dhcp snooping limit .................................. 350
ip dhcp snooping log-invalid ......................... 351
ip dhcp snooping trust .................................. 352
ip dhcp snooping verify mac-address ................. 353
show ip dhcp snooping .................................. 353
show ip dhcp snooping binding ......................... 354
show ip dhcp snooping database ....................... 355
show ip dhcp snooping interfaces .................... 356
show ip dhcp snooping statistics ..................... 357

DHCPv6 Snooping Commands ............................. 359

clear ipv6 dhcp snooping binding .................. 359
clear ipv6 dhcp snooping statistics ................. 360
ipv6 dhcp snooping ...................................... 360
ipv6 dhcp snooping vlan ............................ 361
ipv6 dhcp snooping binding ......................... 362
ipv6 dhcp snooping database .......................... 363
ipv6 dhcp snooping database write-delay ........ 364
ipv6 dhcp snooping limit ................................. 365
ipv6 dhcp snooping log-invalid ...................... 366
ipv6 dhcp snooping trust .................................. 367
ipv6 dhcp snooping verify mac-address ............ 367
ipv6 verify binding ...................................... 368
ipv6 verify source ...................................... 369
show ipv6 dhcp snooping ................................ 370
show ipv6 dhcp snooping binding ...................... 371
show ipv6 dhcp snooping database .................. 372
show ipv6 dhcp snooping interfaces ................. 373
show ipv6 dhcp snooping statistics ................. 373
show ipv6 source binding ............................... 375
show ipv6 verify ......................................... 375
show ipv6 verify source .................................. 376
Dynamic ARP Inspection Commands ................. 378

Commands in this Section ............................... 378
arp ip access-list ....................................... 378
clear ip arp inspection statistics ................. 379
ip arp inspection filter ................................. 380
ip arp inspection limit. .......................... 380
ip arp inspection trust .......................... 381
ip arp inspection validate ...................... 382
ip arp inspection vlan .......................... 383
permit ip host mac host ......................... 384
show arp access-list ............................ 385
show ip arp inspection .......................... 385

**Ethernet Configuration Commands** ............... 389

Commands in this Section ......................... 390
clear counters .................................... 390
description ....................................... 391
default (interface) ................................. 392
duplex .............................................. 393
flowcontrol ....................................... 394
interface .......................................... 395
interface range .................................... 396
link debounce time ................................. 398
rate-limit cpu ..................................... 400
show interfaces ................................... 402
show interfaces advertise ....................... 405
show interfaces configuration .................. 406
service ............................................. 436
ethernet cfm cc level ....................... 436
ethernet cfm mep level .................... 437
ethernet cfm mep enable ................. 438
ethernet cfm mep active ................. 439
ethernet cfm mep archive-hold-time ... 439
ethernet cfm mip level ................... 440
ping ethernet cfm ......................... 441
traceroute ethernet cfm ................. 442
show ethernet cfm errors ............... 443
show ethernet cfm domain .............. 444
show ethernet cfm maintenance-points local 445
show ethernet cfm maintenance-points remote 446
show ethernet cfm statistics .......... 447

**Green Ethernet Commands** ............... 450
Energy-Detect Mode ....................... 450
Energy Efficient Ethernet ............... 450
Commands in this Section ............... 450
green-mode energy-detect .............. 451
green-mode eee ......................... 452
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>green-mode eee { tx-idle-time</td>
<td>tx-wake-time}</td>
</tr>
<tr>
<td>clear green-mode statistics</td>
<td>454</td>
</tr>
<tr>
<td>green-mode eee-lpi-history</td>
<td>454</td>
</tr>
<tr>
<td>show green-mode interface-id</td>
<td>456</td>
</tr>
<tr>
<td>show green-mode</td>
<td>459</td>
</tr>
<tr>
<td>show green-mode eee-lpi-history interface</td>
<td>461</td>
</tr>
</tbody>
</table>

**GMRP Commands** ........................................... 463

Commands in this Section .......................... 464

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmrp enable</td>
<td>464</td>
</tr>
<tr>
<td>clear gmrp statistics</td>
<td>465</td>
</tr>
<tr>
<td>show gmrp configuration</td>
<td>465</td>
</tr>
</tbody>
</table>

**GVRP Commands** ........................................... 467

Commands in this Section ......................... 467

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear gvrp statistics</td>
<td>467</td>
</tr>
<tr>
<td>garp timer</td>
<td>468</td>
</tr>
<tr>
<td>gvrp enable (Global Configuration)</td>
<td>469</td>
</tr>
<tr>
<td>gvrp enable (Interface Configuration)</td>
<td>470</td>
</tr>
<tr>
<td>gvrp registration-forbid</td>
<td>471</td>
</tr>
<tr>
<td>gvrp vlan-creation-forbid</td>
<td>472</td>
</tr>
<tr>
<td>show gvrp configuration</td>
<td>473</td>
</tr>
<tr>
<td>show gvrp error-statistics</td>
<td>474</td>
</tr>
<tr>
<td>show gvrp statistics</td>
<td>475</td>
</tr>
</tbody>
</table>
IGMP Snooping Commands .......................... 477

Commands in this Section .................. 478

ip igmp snooping .......................... 478

show ip igmp snooping .................. 480

show ip igmp snooping groups .. 481

show ip igmp snooping mrouter .... 482

ip igmp snooping vlan immediate-leave .... 483

ip igmp snooping vlan

groupmembership-interval ........ 484

ip igmp snooping vlan

last-member-query-interval .... 485

ip igmp snooping vlan mcrtrexpiretime .... 486

ip igmp snooping report-suppression .... 487

ip igmp snooping unregistered floodall .... 487

ip igmp snooping vlan mrouter .... 488

IGMP Snooping Querier Commands .......... 490

Commands in this Section .................. 490

ip igmp snooping querier ........ 490

ip igmp snooping querier election participate .... 492

ip igmp snooping querier query-interval .... 493

ip igmp snooping querier timer expiry .... 494

ip igmp snooping querier version ... 495
show ip igmp snooping querier. .................. 495

**Interface Error Disable and Auto Recovery ........ 499**

Commands in this Section .................. 499
errdisable recovery cause .................. 499
errdisable recovery interval ............... 501
show errdisable recovery .................. 502
show interfaces status err-disabled .......... 504

**IPv6 Access List Commands .................. 507**

Commands in this Section .................. 507
deny | permit (IPv6 ACL) .................. 508
ipv6 access-list .................. 514
ipv6 access-list rename .................. 515
ipv6 traffic-filter .................. 516
show ipv6 access-lists .................. 517

**IPv6 MLD Snooping Commands ................. 520**

Commands in this Section .................. 520
ipv6 mld snooping vlan

grouppmembership-interval ............... 521
ipv6 mld snooping vlan immediate-leave ........ 521
ipv6 mld snooping

listener-message-suppression ............... 522
ipv6 mld snooping vlan
last-listener-query-interval .................................. 523
ipv6 mld snooping vlan mctrexpiretime ............... 524
ipv6 mld snooping vlan mrouter ......................... 525
ipv6 mld snooping (Global) .............................. 525
show ipv6 mld snooping .................................. 526
show ipv6 mld snooping groups ....................... 528
show ipv6 mld snooping mrouter ...................... 529

**IPv6 MLD Snooping Querier Commands ...............531**

Commands in this Section ................................. 531
ipv6 mld snooping querier .............................. 531
ipv6 mld snooping querier (VLAN mode) ............. 532
ipv6 mld snooping querier address .................... 533
ipv6 mld snooping querier election participate ..... 534
ipv6 mld snooping querier query-interval ........... 534
ipv6 mld snooping querier timer expiry ............... 535
show ipv6 mld snooping querier ....................... 536

**IP Source Guard Commands .........................539**

Commands in this Section ............................... 539
ip verify source ......................................... 539
ip verify binding ....................................... 541
show ip verify ......................................... 541
show ip verify source .................................. 542
show ip source binding ................................ 543

**iSCSI Optimization Commands** .......................... 545

 Commands in this Section ................................. 546

 iscsi cos ................................................. 546

 iscsi enable ............................................. 548

 show iscsi ............................................... 549

**Link Dependency Commands** ............................ 551

 Commands in this Section ................................. 551

 action ..................................................... 551

 link-dependency group .................................. 552

 add .......................................................... 553

 depends-on ............................................. 553

 show link-dependency .................................. 554

**LLDP Commands** ........................................ 556

 Commands in this Section ................................. 557

 clear lldp remote-data .................................. 557

 clear lldp statistics .................................... 558

 dcb enable .............................................. 559

 debug lldp .............................................. 559

 lldp med ................................................. 560

 lldp med confignotification ............................ 561

 lldp med faststartrepeatcount ........................... 561
lldp med transmit-tlv ........................................ 562
lldp notification ............................................. 563
lldp notification-interval ................................. 563
lldp receive .................................................. 564
lldp timers .................................................... 565
lldp transmit .................................................. 566
lldp tlv-select ................................................ 567
show lldp ...................................................... 569
show lldp interface ......................................... 569
show lldp local-device ..................................... 571
show lldp med .................................................. 572
show lldp med interface ..................................... 573
show lldp med local-device detail ....................... 574
show lldp med remote-device ............................. 575
show lldp remote-device ...................................... 577
show lldp statistics ......................................... 579

**Loop Protection** ........................................ 582

Commands in this Section ................................. 582
keepalive (Interface Config) ......................... 582
keepalive (Global Config) ....................... 584
keepalive action ............................................. 585
show keepalive ........................................ 586
show keepalive statistics ...................... 587

**MLAG Commands** ................................ 589

Commands in this Section ..................... 589
clear vpc statistics .......................... 589
feature vpc ...................................... 590
peer detection enable ...................... 591
peer detection interval .................... 591
peer-keepalive destination .............. 592
peer-keepalive enable .................... 594
peer-keepalive timeout ................... 595
role priority .................................. 596
show vpc ....................................... 597
show vpc brief ................................ 598
show vpc consistency-parameters .......... 600
show vpc consistency-features .......... 602
show vpc peer-keepalive .................. 603
show vpc role ................................ 604
show vpc statistics ....................... 605
system-mac .................................... 607
system-priority ................................ 608
Enhanced LAG Hashing ........................................... 630
Manual Aggregation of LAGs ................................. 630
Flexible Assignment of Ports to LAGs ...................... 631
Commands in this Section .................................. 631
channel-group .................................................. 631
interface port-channel ...................................... 632
interface range port-channel ............................... 633
hashing-mode ................................................... 634
lacp port-priority ............................................. 635
lacp system-priority .......................................... 636
lacp timeout ................................................... 637
port-channel local-preference .............................. 638
port-channel min-links ..................................... 639
show interfaces port-channel .............................. 640
show lacp ....................................................... 641
show statistics port-channel ............................... 643

Port Monitor Commands ................................. 646

Commands in this Section .............................. 647
monitor capture (Global Configuration) ............ 647
monitor capture (Privileged Exec) .................. 649
monitor capture mode ..................................... 649
monitor session .......................... 654
remote-span .............................. 659
show monitor capture .................... 660
show monitor session .................... 662
show vlan remote-span .................. 664

**QoS Commands** ............................... 666

Access Control Lists ..................... 666
Layer 2 ACLs ............................... 667
Layer 3/4 IPv4 ACLs ....................... 667
Class of Service (CoS) .................... 667
Queue Mapping ............................. 668
DiffServ ..................................... 669
Commands in this Section ............... 669
assign-queue ............................... 670
class ......................................... 671
class-map ................................... 672
class-map rename ......................... 674
classofservice dot1p-mapping .......... 675
classofservice ip-dscp-mapping ........ 676
classofservice trust ...................... 679
conform-color .............................. 680
cos-queue min-bandwidth .......................... 682

cos-queue random-detect .......................... 684

cos-queue strict ................................. 686

diffserv ........................................... 687

drop ................................................ 688

mark cos ............................................. 689

mark ip-dscp ....................................... 690

mark ip-precedence ................................ 691

match access-group ............................... 692

match class-map ................................... 694

match cos ........................................... 695

match destination-address mac .................... 696

match any ........................................... 697

match dstip ......................................... 698

match dstip6 ....................................... 699

match dstl4port .................................... 700

match ethertype .................................... 700

match ip6flowlbl ................................... 701

match ip dscp ...................................... 702

match ip precedence ............................... 703

match ip tos ....................................... 704
match protocol ........................................ 705
match source-address mac .......................... 707
match srcip ........................................... 708
match srcip6 ........................................... 708
match srcl4port ........................................ 709
match vlan ............................................. 710
mirror ..................................................... 711
police-simple .......................................... 711
police-single-rate ..................................... 713
police-two-rate ........................................ 714
policy-map ............................................. 716
random-detect queue-parms .......................... 717
random-detect
  exponential-weighting-constant .................... 722
redirect ................................................ 723
service-policy ......................................... 724
show class-map ........................................ 725
show classofservice dot1p-mapping ................. 726
show classofservice ip-dscp-mapping ............... 727
show classofservice trust ............................. 729
show diffserv .......................................... 730
show diffserv service interface 731
show diffserv service brief 732
show interfaces cos-queue 733
show interfaces random-detect 735
show policy-map 737
show policy-map interface 737
show service-policy 738
traffic-shape 739
vlan priority 740

**Spanning Tree Commands** 742

Commands in this Section 743
clear spanning-tree detected-protocols 744
exit (mst) 745
instance (mst) 745
name (MST) 747
revision (mst) 748
show spanning-tree 749
show spanning-tree summary 757
show spanning-tree vlan 758
spanning-tree 759
spanning-tree auto-portfast 760
spanning-tree tcnguard ........................................ 780
spanning-tree transmit hold-count ..................... 781
spanning-tree uplinkfast ................................ 782
spanning-tree vlan ............................................. 783
spanning-tree vlan forward-time ....................... 784
spanning-tree vlan hello-time ............................ 785
spanning-tree vlan max-age ............................... 786
spanning-tree vlan root ........................................ 787
spanning-tree vlan priority ................................. 788

**UDLD Commands** ........................................ 790

Detecting Unidirectional Links on a Device

Port ............................................................... 790

Processing UDLD Traffic from Neighbors ............. 791

UDLD in Normal-mode ....................................... 791

UDLD in Aggressive-mode .................................. 791

Commands in this Section .................................. 792

udld enable (Global Configuration) ...................... 792

udld reset ....................................................... 793

udld message time ........................................... 794

udld timeout interval ....................................... 795

udld enable (Interface Configuration) .................. 795
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan</td>
<td>818</td>
</tr>
<tr>
<td>show vlan association mac</td>
<td>820</td>
</tr>
<tr>
<td>show vlan association subnet</td>
<td>821</td>
</tr>
<tr>
<td>show vlan private-vlan</td>
<td>822</td>
</tr>
<tr>
<td>switchport access vlan</td>
<td>823</td>
</tr>
<tr>
<td>switchport dot1q ethertype (Global Configuration)</td>
<td>824</td>
</tr>
<tr>
<td>switchport dot1q ethertype (Interface Configuration)</td>
<td>826</td>
</tr>
<tr>
<td>switchport general forbidden vlan</td>
<td>828</td>
</tr>
<tr>
<td>switchport general acceptable-frame-type</td>
<td>829</td>
</tr>
<tr>
<td>switchport general allowed vlan</td>
<td>830</td>
</tr>
<tr>
<td>switchport general ingress-filtering disable</td>
<td>831</td>
</tr>
<tr>
<td>switchport general pvid</td>
<td>832</td>
</tr>
<tr>
<td>switchport mode</td>
<td>833</td>
</tr>
<tr>
<td>switchport mode dot1q-tunnel</td>
<td>834</td>
</tr>
<tr>
<td>switchport mode private-vlan</td>
<td>836</td>
</tr>
<tr>
<td>switchport private-vlan</td>
<td>837</td>
</tr>
<tr>
<td>switchport trunk</td>
<td>838</td>
</tr>
<tr>
<td>switchport trunk encapsulation dot1q</td>
<td>839</td>
</tr>
</tbody>
</table>
vlan ................................. 840
vlan association mac ......... 841
vlan association subnet ........ 842
vlan makestatic ................. 843
vlan protocol group ............ 843
vlan protocol group add protocol 844
vlan protocol group name ....... 845
vlan protocol group remove .... 846

Switchport Voice VLAN Commands ............. 847

Commands in this Section ............... 848
switchport voice vlan .............. 848
switchport voice vlan (Interface) .... 849
switchport voice vlan priority ........ 853
authentication event server dead action
authorize voice .................... 854
show voice vlan .................... 856

4 Security Commands ..................... 859

AAA Commands .............................. 860

Administrative Authentication ........ 860
Administrative Accounting .......... 861
Accounting Method Lists .......... 862
<table>
<thead>
<tr>
<th>Access Line Modes</th>
<th>862</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Authorization</td>
<td>863</td>
</tr>
<tr>
<td>Network Authentication</td>
<td>863</td>
</tr>
<tr>
<td>Local 802.1x Authentication Server</td>
<td>863</td>
</tr>
<tr>
<td>MAC Authentication Bypass</td>
<td>864</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>865</td>
</tr>
<tr>
<td>Unauthenticated VLAN</td>
<td>865</td>
</tr>
<tr>
<td>Commands in this Section</td>
<td>866</td>
</tr>
<tr>
<td>aaa accounting</td>
<td>867</td>
</tr>
<tr>
<td>aaa accounting delay-start</td>
<td>869</td>
</tr>
<tr>
<td>aaa accounting update</td>
<td>870</td>
</tr>
<tr>
<td>aaa authentication dot1x default</td>
<td>871</td>
</tr>
<tr>
<td>aaa authentication enable</td>
<td>872</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>874</td>
</tr>
<tr>
<td>aaa authorization</td>
<td>876</td>
</tr>
<tr>
<td>aaa authorization network default radius</td>
<td>880</td>
</tr>
<tr>
<td>aaa ias-user username</td>
<td>881</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>881</td>
</tr>
<tr>
<td>aaa server radius dynamic-author</td>
<td>882</td>
</tr>
<tr>
<td>authentication enable</td>
<td>884</td>
</tr>
<tr>
<td>authentication order</td>
<td>885</td>
</tr>
</tbody>
</table>
username ................................................. 904
username unlock .................................. 907

Administrative Profiles Commands ..............909

Commands in this Section ......................... 910
admin-profile .......................................... 910
description (Administrative Profile Configuration) . 911
rule .......................................................... 912
show admin-profiles .................................. 913
show admin-profiles brief ......................... 914
show cli modes .......................................... 915

E-mail Alerting Commands .........................916

Commands in this Section ......................... 916
logging email ........................................... 917
logging email urgent ............................... 918
logging email message-type to-addr .......... 919
logging email from-addr ......................... 920
logging email message-type subject ....... 921
logging email logtime ............................ 922
logging email test message-type .......... 923
show logging email statistics ................ 923
clear logging email statistics ................ 924
security .................................................. 925
mail-server ip-address | hostname .................................. 925
port (Mail Server Configuration Mode) ........... 926
username (Mail Server Configuration Mode) .... 927
password (Mail Server Configuration Mode) .... 928
show mail-server ........................................... 929

RADIUS Commands ................................. 931
RADIUS-based Dynamic VLAN Assignment .... 931
RADIUS Change of Authorization. ............... 932
Commands in this Section ............................... 933
acct-port ..................................................... 934
attribute 6 .................................................. 935
attribute 8 .................................................. 936
attribute 25 ............................................... 937
attribute 31 ............................................... 938
attribute 168 include-in-access-req .............. 939
authentication event fail retry .................... 940
auth-port ..................................................... 942
automate-tester .......................................... 943
deadtime .................................................... 944
key .......................................................... 945
msgauth ...................................................... 946
name (RADIUS Server) ................................. 947
primary .............................................. 948
priority .............................................. 949
radius server attribute 4 ......................... 950
radius server attribute 6 ......................... 951
radius server attribute 8 ......................... 952
radius server attribute 25 ......................... 953
radius server attribute 31 ......................... 954
radius server attribute 168 ....................... 956
radius server deadtime ......................... 957
radius server ........................................ 958
radius server key .................................. 960
radius server retransmit ....................... 961
radius server source-ip ......................... 962
radius server source-interface .................. 963
radius server timeout ......................... 964
radius server vsa send authentication ........ 964
retransmit .......................................... 967
show aaa servers .................................. 968
show radius statistics ............................ 971
source-ip .......................................... 974
timeout ........................................... 975
usage ............................................ 976

**TACACS+ Commands** .............................. 977

Commands in this Section ....................... 977
key ................................................. 978
port ................................................. 979
priority ......................................... 980
show tacacs ....................................... 980
tacacs-server host ............................... 981
tacacs-server key ................................. 982
tacacs-server source-interface ............... 983
tacacs-server timeout ......................... 984
timeout ......................................... 985

**802.1x Commands** ................................. 987

802.1x Monitor Mode ......................... 987

Commands in this Section ....................... 988
dot1x dynamic-vlan enable .................... 989
dot1x eapolflood .............................. 990
dot1x initialize ................................. 991
mab ................................................. 991
default mab ....................................... 992
mab request format ............................. 994
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x interface</td>
<td>1020</td>
</tr>
<tr>
<td>show dot1x interface statistics</td>
<td>1022</td>
</tr>
<tr>
<td>show dot1x users</td>
<td>1023</td>
</tr>
<tr>
<td>clear dot1x authentication-history</td>
<td>1024</td>
</tr>
<tr>
<td>dot1x guest-vlan</td>
<td>1025</td>
</tr>
<tr>
<td>dot1x timeout guest-vlan-period</td>
<td>1026</td>
</tr>
<tr>
<td>dot1x unauth-vlan</td>
<td>1027</td>
</tr>
<tr>
<td>show dot1x advanced</td>
<td>1028</td>
</tr>
</tbody>
</table>

### Captive Portal Commands 1030

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication timeout</td>
<td>1032</td>
</tr>
<tr>
<td>captive-portal</td>
<td>1032</td>
</tr>
<tr>
<td>enable</td>
<td>1033</td>
</tr>
<tr>
<td>http port</td>
<td>1034</td>
</tr>
<tr>
<td>https port</td>
<td>1034</td>
</tr>
<tr>
<td>show captive-portal</td>
<td>1035</td>
</tr>
<tr>
<td>show captive-portal status</td>
<td>1036</td>
</tr>
<tr>
<td>block</td>
<td>1037</td>
</tr>
<tr>
<td>configuration</td>
<td>1037</td>
</tr>
<tr>
<td>enable</td>
<td>1038</td>
</tr>
<tr>
<td>group</td>
<td>1039</td>
</tr>
</tbody>
</table>
interface ............................................. 1039
locale ............................................. 1040
name (Captive Portal) ......................... 1041
protocol ........................................... 1041
redirect ............................................ 1042
redirect-url ...................................... 1042
session-timeout ................................. 1043
verification ...................................... 1044
captive-portal client deauthenticate .... 1045
show captive-portal client status ........ 1045
show captive-portal configuration client
status ............................................. 1046
show captive-portal interface client status . 1047
show captive-portal interface configuration
status ............................................. 1048
clear captive-portal users ................. 1049
no user .......................................... 1050
show captive-portal user ................. 1050
user group ...................................... 1051
user-logout .................................... 1052
user name ...................................... 1053
user password ............................................. 1054
user session-timeout .......................... 1054
show captive-portal configuration ........... 1055
show captive-portal configuration interface . 1056
show captive-portal configuration locales 1057
show captive-portal configuration status 1058
user group ............................................. 1059
user group moveusers .......................... 1059
user group name ................................... 1060

**Denial of Service Commands** ......................1061

Commands in this Section ....................... 1062
dos-control firstfrag .......................... 1063
dos-control icmp ................................. 1063
dos-control l4port ............................... 1064
dos-control sipdip ............................... 1065
dos-control tcpflag ............................... 1066
dos-control tcpfrag ................................ 1066
rate-limit cpu ................................. 1067
show dos-control ................................. 1069
show system internal pktmgr .................... 1070
storm-control broadcast .......................... 1071
crypto key generate dsa .................................. 1103
crypto key generate rsa .................................. 1104
crypto key pubkey-chain ssh ............................ 1105
crypto key zeroize pubkey-chain ...................... 1106
crypto key zeroize \{rsa\|dsa\} .......................... 1107
ip ssh port .............................................. 1108
ip ssh pubkey-auth ..................................... 1109
ip ssh server .......................................... 1110
key-string ............................................. 1111
show crypto key mypubkey .............................. 1112
show crypto key pubkey-chain ssh .................. 1113
show ip ssh ............................................ 1114

5 Audio Visual Bridging Commands ........ 1117

Multiple MAC Registration Protocol Commands .......................................................... 1118

Commands in this Section ......................... 1118
clear mmrp statistics ................................. 1118
mmrp .................................................... 1119
mmrp global ............................................ 1120
mmrp periodic state machine ...................... 1121
show mmrp ............................................. 1122
show mmrp statistics .......................... 1123

**Multiple VLAN Registration Protocol Commands** .......................................................... 1125

Commands in this Section .......................... 1125
clear mvrp statistics ............................ 1125
mvrp ............................................. 1126
mvrp global ....................................... 1127
mvrp periodic state machine .................... 1128
show mvrp ......................................... 1129
show mvrp statistics ............................. 1130

**Multiple Stream Reservation Protocol Commands** ...................................................... 1132

Commands in this Section .......................... 1132
clear msrp statistics ............................ 1132
msrp (Interface) ................................ 1133
msrp boundary-propagate ....................... 1134
msrp delta-bw ................................... 1135
msrp global ....................................... 1136
msrp max-fan-in-ports ........................... 1137
msrp srclass-pvid ................................ 1138
msrp srclassqav .................................. 1139
msrp talker-pruning ............................... 1141
show msrp ........................................ 1142
show msrp reservations .................................. 1145
show msrp statistics .................................. 1146
show msrp stream .................................. 1148

802.1AS Timesync Commands ..........................1151
Commands in this Section .......................... 1151
clear dot1as statistics ......................... 1151
dot1as (Global Configuration) .................. 1152
dot1as (Interface Configuration) .............. 1153
dot1as priority .................................. 1154
dot1as interval announce ...................... 1155
dot1as interval sync ......................... 1157
dot1as interval pdelay ...................... 1158
dot1as timeout announce ...................... 1159
dot1as timeout sync ......................... 1161
dot1as pdelay-threshold ...................... 1162
dot1as interval pdelay-loss .............. 1163
show dot1as .................................. 1165
show dot1as statistics ...................... 1168

6 Data Center Technology Commands .... 1171

Data Center Bridging Commands .............. 1172

Data Center Bridging Exchange Protocol .... 1172
Interoperability with IEEE DCBX .......................... 1176
Port Roles ..................................................... 1176
Commands in this Section .................................. 1180
Data Center Bridging Capability Exchange
Commands ...................................................... 1180
datacenter-bridging ......................................... 1180
lldp dcbx version .............................................. 1181
lldp dcbx port-role ........................................... 1182
show lldp tlv-select .......................................... 1184
show lldp dcbx ................................................ 1185
Enhanced Transmission Selection (ETS)
Commands ...................................................... 1189
classofservice traffic-class-group ...................... 1189
traffic-class-group max-bandwidth .................... 1190
traffic-class-group min-bandwidth .................... 1192
traffic-class-group strict ............................... 1193
traffic-class-group weight ............................... 1195
show classofservice traffic-class-group ............. 1196
show interfaces traffic ..................................... 1197
show interfaces traffic-class-group .................. 1199
OpenFlow Commands ....................................... 1201

OpenFlow Commands .......................... 1201
arp dynamicrenew ........................................ 1234
arp purge ................................................. 1235
arp resptime .............................................. 1236
arp retries ............................................... 1237
arp timeout .............................................. 1237
clear arp-cache ........................................ 1238
clear arp-cache management ....................... 1239
ip local-proxy-arp ....................................... 1240
ip proxy-arp ............................................. 1240
show arp .................................................. 1241

Bidirectional Forwarding Detection Commands ............................................. 1243

Border Gateway Protocol Commands ..................... 1254
Commands in this Section .................. 1254

router bgp .................. 1257

address-family .................. 1258

address-family ipv4 vrf ............... 1260

address-family ipv6 .................. 1261

address-family vpnv4 unicast ........... 1261

aggregate-address .................. 1263

bgp aggregate-different-meds (BGP Router Configuration) .................. 1264

bgp aggregate-different-meds (IPv6 Address Family Configuration) ............... 1265

bgp always-compare-med .................. 1266

bgp client-to-client reflection (BGP Router Configuration) .................. 1267

bgp client-to-client reflection (IPv6 Address Family Configuration) ............... 1268

bgp cluster-id .................. 1269

bgp default local-preference ............... 1270

bgp fast-external-fallover ............... 1271

bgp fast-internal-fallover ............... 1272

bgp listen .................. 1273
bgp log-neighbor-changes .......................... 1275
bgp maxas-limit ........................................ 1275
bgp router-id ............................................ 1276
clear ip bgp ............................................. 1277
clear ip bgp counters ................................... 1279
default-information originate (BGP Router
Configuration) ............................................ 1279
default-information originate (IPv6 Address
Family Configuration) .................................. 1280
default metric (BGP Router Configuration) .... 1281
default metric (IPv6 Address Family
Configuration) ............................................ 1282
distance .................................................... 1283
distance bgp (BGP Router Configuration) ....... 1284
distance bgp (IPv6 Address Family
Configuration) ............................................ 1285
distribute-list prefix in ................................. 1287
distribute-list prefix out (BGP Router
Configuration) ............................................ 1287
distribute-list prefix out (IPv6 Address Family
Configuration) ............................................ 1288
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor default-originate (BGP Router Configuration)</td>
<td>1310</td>
</tr>
<tr>
<td>neighbor default-originate (IPv6 Address Family Configuration)</td>
<td>1311</td>
</tr>
<tr>
<td>neighbor description</td>
<td>1313</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>1314</td>
</tr>
<tr>
<td>neighbor filter-list (BGP Router Configuration)</td>
<td>1316</td>
</tr>
<tr>
<td>neighbor filter-list (IPv6 Address Family Configuration)</td>
<td>1318</td>
</tr>
<tr>
<td>neighbor inherit peer</td>
<td>1319</td>
</tr>
<tr>
<td>neighbor local-as</td>
<td>1320</td>
</tr>
<tr>
<td>neighbor maximum-prefix (BGP Router Configuration)</td>
<td>1322</td>
</tr>
<tr>
<td>neighbor maximum-prefix (IPv6 Address Family Configuration)</td>
<td>1324</td>
</tr>
<tr>
<td>neighbor next-hop-self (BGP Router Configuration)</td>
<td>1325</td>
</tr>
<tr>
<td>neighbor next-hop-self (IPv6 Address Family Configuration)</td>
<td>1326</td>
</tr>
<tr>
<td>neighbor password</td>
<td>1327</td>
</tr>
</tbody>
</table>
neighbor prefix-list (BGP Router Configuration) ........................................... 1329
neighbor prefix-list (IPv6 Address Family Configuration) ................................. 1330
neighbor remote-as ................................................................. 1331
neighbor remove-private-as ........................................................ 1332
neighbor rfc5549-support .......................................................... 1333
neighbor route-map (BGP Router Configuration) ......................................... 1335
neighbor route-map (IPv6 Address Family Configuration) .............................. 1336
neighbor route-reflector-client (BGP Router Configuration) .............................. 1337
neighbor route-reflector-client (IPv6 Address Family Configuration) ............... 1338
neighbor send-community (BGP Router Configuration) .................................. 1340
neighbor send-community (IPv6 Address Family Configuration) ...................... 1341
neighbor shutdown ................................................................. 1342
neighbor timers ................................................................. 1343
show bgp ipv6 route-reflection .......................... 1384
show ip bgp ............................................. 1385
show ip bgp aggregate-address ...................... 1387
show ip bgp community ............................... 1388
show ip bgp community-list ......................... 1389
show ip bgp extcommunity-list .................... 1390
show ip bgp listen range ............................ 1391
show ip bgp neighbors ............................... 1392
show ip bgp neighbors advertised-routes .......... 1399
show ip bgp neighbors received-routes .......... 1401
show ip bgp neighbors policy ....................... 1403
show ip bgp route-reflection ....................... 1404
show ip bgp statistics ............................... 1405
show ip bgp summary .................................. 1407
show ip bgp template .................................. 1410
show ip bgp traffic .................................... 1411
show ip bgp update-group ......................... 1413
show ip bgp vpn4 ..................................... 1417
template peer .......................................... 1421
timers bgp .............................................. 1423

BGP Routing Policy ........................................ 1425
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip as-path access-list</td>
<td>1426</td>
</tr>
<tr>
<td>ip bgp-community new-format</td>
<td>1428</td>
</tr>
<tr>
<td>ip community-list</td>
<td>1429</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>1430</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>1432</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>1433</td>
</tr>
<tr>
<td>match as-path</td>
<td>1436</td>
</tr>
<tr>
<td>match community</td>
<td>1437</td>
</tr>
<tr>
<td>match ip address prefix-list</td>
<td>1438</td>
</tr>
<tr>
<td>match ipv6 address prefix-list</td>
<td>1439</td>
</tr>
<tr>
<td>show ip as-path-access-list</td>
<td>1440</td>
</tr>
<tr>
<td>show ip community-list</td>
<td>1441</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>1442</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>1444</td>
</tr>
<tr>
<td>clear ip prefix-list</td>
<td>1446</td>
</tr>
<tr>
<td>clear ipv6 prefix-list</td>
<td>1447</td>
</tr>
<tr>
<td>clear ip community-list</td>
<td>1448</td>
</tr>
<tr>
<td>set as-path</td>
<td>1449</td>
</tr>
<tr>
<td>set comm-list delete</td>
<td>1450</td>
</tr>
<tr>
<td>set community</td>
<td>1451</td>
</tr>
</tbody>
</table>
set ipv6 next-hop (BGP) .......................... 1452
set local-preference ............................ 1453
set metric ............................. 1454

**DVMRP Commands** ................................. 1456

Commands in this Section .......................... 1456
ip dvmrp ........................................ 1456
ip dvmrp metric ................................ 1457
show ip dvmrp .................................. 1458
show ip dvmrp interface ......................... 1459
show ip dvmrp neighbor ......................... 1459
show ip dvmrp nexthop ......................... 1460
show ip dvmrp prune ................... 1461
show ip dvmrp route ..................... 1462

**IGMP Commands** ................................. 1463

Commands in this Section .......................... 1464
ip igmp last-member-query-count ........... 1464
ip igmp last-member-query-interval ........ 1465
ip igmp mroute-proxy ......................... 1466
ip igmp query-interval .................... 1467
ip igmp query-max-response-time .......... 1468
ip igmp robustness ...................... 1469
ip igmp startup-query-count ........... 1469
ip igmp startup-query-interval .................. 1470
ip igmp version ................................. 1471
show ip igmp ...................................... 1472
show ip igmp groups ............................... 1472
show ip igmp interface ............................ 1473
show ip igmp membership ......................... 1474
show ip igmp interface stats ..................... 1475

**IGMP Proxy Commands** ..........................1477

Commands in this Section ......................... 1477
ip igmp proxy-service. ........................... 1477
ip igmp proxy-service reset-status ............... 1478
ip igmp proxy-service unsolicit-rprt-interval .... 1479
show ip igmp proxy-service ....................... 1480
show ip igmp proxy-service interface ............ 1481
show ip igmp-proxy groups ......................... 1481
show ip igmp proxy-service groups detail ........ 1482

**IP Helper/DHCP Relay Commands** ..............1484

Commands in this Section ......................... 1486
bootpdhcprelay maxhopcount ...................... 1487
bootpdhcprelay minwaittime ....................... 1488
clear ip helper statistics ......................... 1489
ip dhcp relay information check ................... 1489
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route default</td>
<td>1515</td>
</tr>
<tr>
<td>ip route distance</td>
<td>1517</td>
</tr>
<tr>
<td>ip routing</td>
<td>1518</td>
</tr>
<tr>
<td>ip unnumbered</td>
<td>1519</td>
</tr>
<tr>
<td>ip unnumbered gratuitous-arp accept</td>
<td>1520</td>
</tr>
<tr>
<td>ip unreachable</td>
<td>1521</td>
</tr>
<tr>
<td>match ip address</td>
<td>1522</td>
</tr>
<tr>
<td>match length</td>
<td>1525</td>
</tr>
<tr>
<td>match mac-list</td>
<td>1526</td>
</tr>
<tr>
<td>route-map</td>
<td>1527</td>
</tr>
<tr>
<td>set interface null0</td>
<td>1529</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>1530</td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>1531</td>
</tr>
<tr>
<td>set ip precedence</td>
<td>1532</td>
</tr>
<tr>
<td>show ip brief</td>
<td>1533</td>
</tr>
<tr>
<td>show ip interface</td>
<td>1534</td>
</tr>
<tr>
<td>show ip policy</td>
<td>1535</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>1536</td>
</tr>
<tr>
<td>show ip route</td>
<td>1540</td>
</tr>
<tr>
<td>show ip route static</td>
<td>1543</td>
</tr>
<tr>
<td>show ip route preferences</td>
<td>1543</td>
</tr>
</tbody>
</table>
show ip route summary. .......................... 1544
show ip traffic. ................................. 1546
show ip vlan ................................. 1548
show route-map ................................. 1548
show routing heap summary .......................... 1551

IPv6 Routing Commands .......................... 1553

IPv6 Limitations & Restrictions ...................... 1553

Commands in this Section ......................... 1553
clear ipv6 neighbors ............................. 1554
clear ipv6 statistics ............................. 1555
ipv6 address ............................. 1556
ipv6 enable ............................. 1557
ipv6 hop-limit ............................. 1558
ipv6 host ............................. 1558
ipv6 icmp error-interval ......................... 1559
ipv6 mld last-member-query-count .................. 1560
ipv6 mld last-member-query-interval .................. 1561
ipv6 mld host-proxy .......................... 1561
ipv6 mld host-proxy reset-status .................. 1562
ipv6 mld host-proxy unsolicit-rprt-interval ............ 1563
ipv6 mld query-interval ......................... 1563
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld query-max-response-time</td>
<td>1564</td>
</tr>
<tr>
<td>ipv6 nd dad attempts</td>
<td>1565</td>
</tr>
<tr>
<td>ipv6 nd ra hop-limit unspecified</td>
<td>1566</td>
</tr>
<tr>
<td>ipv6 nd managed-config-flag</td>
<td>1566</td>
</tr>
<tr>
<td>ipv6 nd ns-interval</td>
<td>1567</td>
</tr>
<tr>
<td>ipv6 nd nud max-multicast-solicits</td>
<td>1568</td>
</tr>
<tr>
<td>ipv6 nd nud max-unicast-solicits</td>
<td>1569</td>
</tr>
<tr>
<td>ipv6 nd nud retry</td>
<td>1570</td>
</tr>
<tr>
<td>ipv6 nd other-config-flag</td>
<td>1571</td>
</tr>
<tr>
<td>ipv6 nd prefix</td>
<td>1572</td>
</tr>
<tr>
<td>ipv6 nd raguard attach-policy</td>
<td>1573</td>
</tr>
<tr>
<td>ipv6 nd ra-interval</td>
<td>1574</td>
</tr>
<tr>
<td>ipv6 nd ra-lifetime</td>
<td>1575</td>
</tr>
<tr>
<td>ipv6 nd reachable-time</td>
<td>1576</td>
</tr>
<tr>
<td>ipv6 nd suppress-ra.</td>
<td>1577</td>
</tr>
<tr>
<td>ipv6 redirect</td>
<td>1577</td>
</tr>
<tr>
<td>ipv6 route</td>
<td>1578</td>
</tr>
<tr>
<td>ipv6 route distance</td>
<td>1580</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>1581</td>
</tr>
<tr>
<td>ipv6 unreachable</td>
<td>1581</td>
</tr>
<tr>
<td>show ipv6 brief</td>
<td>1582</td>
</tr>
</tbody>
</table>
show ipv6 interface . . . . . . . . . . . . . . . . 1583
show ipv6 mld groups . . . . . . . . . . . . . . . . 1585
show ipv6 mld interface . . . . . . . . . . . . . . . 1587
show ipv6 mld host-proxy . . . . . . . . . . . . . . 1590
show ipv6 mld host-proxy groups . . . . . . . . . 1591
show ipv6 mld host-proxy groups detail . . . . . 1592
show ipv6 mld host-proxy interface . . . . . . . . 1594
show ipv6 mld traffic . . . . . . . . . . . . . . . . . 1595
show ipv6 nd raguard policy . . . . . . . . . . . . . 1596
show ipv6 neighbors . . . . . . . . . . . . . . . . . 1598
show ipv6 protocols . . . . . . . . . . . . . . . . . . 1598
show ipv6 route . . . . . . . . . . . . . . . . . . . . 1600
show ipv6 route preferences . . . . . . . . . . . . . 1601
show ipv6 route summary . . . . . . . . . . . . . . 1602
show ipv6 snooping counters . . . . . . . . . . . . . 1603
show ipv6 traffic . . . . . . . . . . . . . . . . . . . . 1604
show ipv6 vlan . . . . . . . . . . . . . . . . . . . . . 1605
traceroute ipv6 . . . . . . . . . . . . . . . . . . . . . 1606

Loopback Interface Commands .................1608

Commands in this Section . . . . . . . . . . . . . . 1608
interface loopback . . . . . . . . . . . . . . . . . . . 1608
show interfaces loopback ............... 1609

**IP Multicast Commands** .....................1611

Commands in this Section .................. 1612
clear ip mroute ......................... 1612
ip multicast boundary .................. 1614
ip mroute ......................... 1614
ip multicast-routing .................. 1615
ip multicast ttl-threshold ............. 1617
ip pim .................................. 1617
ip pim bsr-border ..................... 1618
ip pim bsr-candidate ................. 1619
ip pim dense-mode .................. 1620
ip pim dr-priority .................. 1621
ip pim hello-interval .................. 1621
ip pim join-prune-interval ............ 1622
ip pim rp-address .................. 1623
ip pim rp-candidate .................. 1624
ip pim sparse-mode .................. 1625
ip pim ssm ......................... 1626
show ip mfc ......................... 1626
show ip multicast .................. 1628
show ip pim boundary .......... 1628
show ip multicast interface. .......... 1629
show ip mroute .................. 1630
show ip mroute group .............. 1631
show ip mroute source ............ 1631
show ip mroute static. ............. 1632
show ip pim ...................... 1633
show ip pim bsr-router ............ 1634
show ip pim interface ............. 1635
show ip pim neighbor .............. 1637
show ip pim rp-hash .............. 1638
show ip pim rp mapping .......... 1639
show ip pim statistics .......... 1640

**IPv6 Multicast Commands ..................** 1642

clear ipv6 mroute .................. 1642
ipv6 pim (VLAN Interface config). .......... 1643
ipv6 pim bsr-border ............... 1644
ipv6 pim bsr-candidate .......... 1645
ipv6 pim dense-mode ............... 1646
ipv6 pim dr-priority .............. 1646
ipv6 pim hello-interval .......... 1647
Graceful Restart ............................................. 1668
Commands in this Section .......................... 1668
area default-cost (Router OSPF) ............... 1669
area nssa (Router OSPF) ....................... 1670
area nssa default-info-originate (Router OSPF
Config) .................................................. 1672
area nssa no-redistribute ....................... 1673
area nssa no-summary ............................ 1673
area nssa translator-role ...................... 1674
area nssa translator-stab-intv ............... 1675
area range (Router OSPF) ...................... 1676
area stub ................................................. 1678
area stub no-summary ......................... 1679
area virtual-link ..................................... 1680
area virtual-link authentication ........... 1683
area virtual-link dead-interval ............ 1684
area virtual-link hello-interval ........... 1685
area virtual-link retransmit-interval .... 1686
area virtual-link transmit-delay .......... 1687
auto-cost ............................................... 1687
bandwidth ............................................. 1688
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd</td>
<td>1689</td>
</tr>
<tr>
<td>capability opaque</td>
<td>1690</td>
</tr>
<tr>
<td>clear ip ospf</td>
<td>1691</td>
</tr>
<tr>
<td>clear ip ospf stub-router</td>
<td>1692</td>
</tr>
<tr>
<td>compatible rfc1583</td>
<td>1693</td>
</tr>
<tr>
<td>default-information originate (Router OSPF Configuration)</td>
<td>1693</td>
</tr>
<tr>
<td>default-metric</td>
<td>1695</td>
</tr>
<tr>
<td>distance ospf</td>
<td>1695</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>1696</td>
</tr>
<tr>
<td>enable</td>
<td>1697</td>
</tr>
<tr>
<td>exit-overflow-interval</td>
<td>1698</td>
</tr>
<tr>
<td>external-lsdb-limit</td>
<td>1699</td>
</tr>
<tr>
<td>ip ospf area</td>
<td>1700</td>
</tr>
<tr>
<td>ip ospf authentication</td>
<td>1701</td>
</tr>
<tr>
<td>ip ospf cost</td>
<td>1702</td>
</tr>
<tr>
<td>ip ospf database-filter all out</td>
<td>1702</td>
</tr>
<tr>
<td>ip ospf dead-interval</td>
<td>1703</td>
</tr>
<tr>
<td>ip ospf hello-interval</td>
<td>1704</td>
</tr>
<tr>
<td>ip ospf mtu-ignore</td>
<td>1704</td>
</tr>
<tr>
<td>ip ospf network</td>
<td>1705</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ip ospf priority</td>
<td>1706</td>
</tr>
<tr>
<td>ip ospf retransmit-interval</td>
<td>1707</td>
</tr>
<tr>
<td>ip ospf transmit-delay</td>
<td>1708</td>
</tr>
<tr>
<td>log adjacency-changes</td>
<td>1708</td>
</tr>
<tr>
<td>max-metric router-lsa</td>
<td>1709</td>
</tr>
<tr>
<td>maximum-paths</td>
<td>1711</td>
</tr>
<tr>
<td>network area</td>
<td>1712</td>
</tr>
<tr>
<td>nsf</td>
<td>1713</td>
</tr>
<tr>
<td>nsf helper</td>
<td>1714</td>
</tr>
<tr>
<td>nsf helper strict-lsa-checking</td>
<td>1715</td>
</tr>
<tr>
<td>nsf restart-interval</td>
<td>1715</td>
</tr>
<tr>
<td>passive-interface default</td>
<td>1716</td>
</tr>
<tr>
<td>passive-interface</td>
<td>1717</td>
</tr>
<tr>
<td>redistribute (OSPF)</td>
<td>1718</td>
</tr>
<tr>
<td>router-id</td>
<td>1719</td>
</tr>
<tr>
<td>router ospf</td>
<td>1720</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>1721</td>
</tr>
<tr>
<td>show ip ospf abr</td>
<td>1727</td>
</tr>
<tr>
<td>show ip ospf area</td>
<td>1728</td>
</tr>
<tr>
<td>show ip ospf asbr</td>
<td>1730</td>
</tr>
<tr>
<td>show ip ospf database</td>
<td>1731</td>
</tr>
</tbody>
</table>
show ip ospf database database-summary
show ip ospf interface

. . .

1734

. . . . . . . . . . . . . .

1736

show ip ospf interface brief

. . . . . . . . . . .

1738

show ip ospf interface stats

. . . . . . . . . . .

1739

. . . . . . . . . . . . .

1739

. . . . . . . . . . . . . .

1741

. . . . . . . . . . . . . . . .

1745

show ip ospf lsa-group .
show ip ospf neighbor
show ip ospf range

show ip ospf statistics

. . . . . . . . . . . . . .
. . . . . . . . . . . . .

1748

. . . . . . . . . . . . . . .

1749

show ip ospf stub table .
show ip ospf traffic .

show ip ospf virtual-links .

. . . . . . . . . . . .

show ip ospf virtual-links brief
timers pacing flood .

1751

. . . . . . . . . .

1752

. . . . . . . . . . . . . . .

1753

timers pacing lsa-group
timers spf

1746

. . . . . . . . . . . . .

1754

. . . . . . . . . . . . . . . . . . . . .

1755

OSPFv3 Commands . . . . . . . . . . . . . . . . . . . . . . . . . . .1756
area default-cost (Router OSPFv3) .
area nssa (Router OSPFv3) .

. . . . . . .

1757

. . . . . . . . . . .

1758

area nssa default-info-originate (Router OSPFv3
Config)

. . . . . . . . . . . . . . . . . . . . . .

area nssa no-redistribute.

. . . . . . . . . . . .

1759
1760

Contents

71


<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>area nssa no-summary</td>
<td>1761</td>
</tr>
<tr>
<td>area nssa translator-role</td>
<td>1762</td>
</tr>
<tr>
<td>area nssa translator-stab-intv</td>
<td>1763</td>
</tr>
<tr>
<td>area range (Router OSPFv3)</td>
<td>1764</td>
</tr>
<tr>
<td>area stub</td>
<td>1765</td>
</tr>
<tr>
<td>area stub no-summary</td>
<td>1766</td>
</tr>
<tr>
<td>area virtual-link</td>
<td>1766</td>
</tr>
<tr>
<td>area virtual-link dead-interval</td>
<td>1768</td>
</tr>
<tr>
<td>area virtual-link hello-interval</td>
<td>1769</td>
</tr>
<tr>
<td>area virtual-link retransmit-interval</td>
<td>1770</td>
</tr>
<tr>
<td>area virtual-link transmit-delay</td>
<td>1771</td>
</tr>
<tr>
<td>default-information originate (Router OSPFv3 Configuration)</td>
<td>1771</td>
</tr>
<tr>
<td>default-metric</td>
<td>1772</td>
</tr>
<tr>
<td>distance ospf</td>
<td>1773</td>
</tr>
<tr>
<td>enable</td>
<td>1774</td>
</tr>
<tr>
<td>exit-overflow-interval</td>
<td>1775</td>
</tr>
<tr>
<td>external-lsdb-limit</td>
<td>1776</td>
</tr>
<tr>
<td>ipv6 ospf</td>
<td>1776</td>
</tr>
<tr>
<td>ipv6 ospf area</td>
<td>1777</td>
</tr>
<tr>
<td>ipv6 ospf cost</td>
<td>1778</td>
</tr>
</tbody>
</table>
Routing Information Protocol Commands  ........1821

Commands in this Section ................. 1821
auto-summary ............................. 1821
default-information originate (Router RIP Configuration) ...................... 1822
default-metric ............................ 1823
distance rip ............................... 1824
distribute-list out ......................... 1824
enable ..................................... 1825
hostroutesaccept ......................... 1826
ip rip .................................... 1827
ip rip authentication ........................ 1827
ip rip receive version .................... 1828
ip rip send version ....................... 1829
redistribute (RIP) ......................... 1830
router rip ................................ 1831
show ip rip ................................ 1832
show ip rip interface ...................... 1833
show ip rip interface brief ............... 1834
split-horizon ................................ 1835

Tunnel Interface Commands ................1836
Commands in this Section

interface tunnel ........................................... 1836
show interfaces tunnel .................................. 1837
tunnel destination ....................................... 1838
tunnel mode ipv6ip ........................................ 1839
tunnel source ............................................. 1839

Virtual Router Commands ................................. 1841

Commands in this Section ................................. 1842
description .................................................... 1843
ip vrf ............................................................ 1844
ip vrf forwarding ......................................... 1845
maximum routes ............................................ 1846
show ip vrf ..................................................... 1847

Virtual Router Redundancy Protocol
Commands ..................................................... 1850

Pingable VRRP Interface .................................. 1850
VRRP Route/Interface Tracking .......................... 1851
Interface Tracking ......................................... 1852
Route Tracking ............................................. 1852
Commands in this Section ................................. 1852
ip vrrp .......................................................... 1853
vrrp accept-mode ......................................... 1853
vrrp authentication ........................................ 1854
vrrp description ........................................... 1855
vrrp ip ....................................................... 1856
vrrp mode ................................................... 1857
vrrp preempt ............................................... 1858
vrrp priority ................................................. 1859
vrrp timers advertise ...................................... 1859
vrrp timers learn .......................................... 1860
vrrp track interface ....................................... 1861
vrrp track ip route ........................................ 1862
show vrrp .................................................... 1863
show vrrp interface ........................................ 1865

8 Switch Management Commands ............. 1869

Application Deployment ............................. 1870

Commands in this Section ......................... 1870
application install ...................................... 1870
application start ....................................... 1871
application stop ........................................ 1872
show application ........................................ 1873

Auto-Install Commands ............................. 1875

Commands in this Section ......................... 1876
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sntp configuration</td>
<td>1892</td>
</tr>
<tr>
<td>show sntp server</td>
<td>1893</td>
</tr>
<tr>
<td>show sntp status</td>
<td>1894</td>
</tr>
<tr>
<td>sntp authenticate</td>
<td>1895</td>
</tr>
<tr>
<td>sntp authentication-key</td>
<td>1896</td>
</tr>
<tr>
<td>sntp broadcast client enable</td>
<td>1897</td>
</tr>
<tr>
<td>sntp client poll timer</td>
<td>1897</td>
</tr>
<tr>
<td>sntp server</td>
<td>1898</td>
</tr>
<tr>
<td>sntp source-interface</td>
<td>1899</td>
</tr>
<tr>
<td>sntp trusted-key</td>
<td>1900</td>
</tr>
<tr>
<td>sntp unicast client enable</td>
<td>1901</td>
</tr>
<tr>
<td>clock set</td>
<td>1902</td>
</tr>
<tr>
<td>clock timezone hours-offset</td>
<td>1902</td>
</tr>
<tr>
<td>no clock timezone</td>
<td>1903</td>
</tr>
<tr>
<td>clock summer-time recurring</td>
<td>1904</td>
</tr>
<tr>
<td>clock summer-time date</td>
<td>1905</td>
</tr>
<tr>
<td>no clock summer-time</td>
<td>1906</td>
</tr>
<tr>
<td>show clock</td>
<td>1906</td>
</tr>
</tbody>
</table>

**Command Line Configuration Scripting**

**Commands** .................................................. 1908

Commands in this Section .......................... 1908

script apply ............................................. 1908
Configuration and Image File Commands

File System Commands
Command Line Interface Scripting
Commands in this Section

boot system

clear config

copy

delete
dir

erase

copiedescr.

rename

show backup-config

show bootvar

show running-config

show startup-config

write

DHCP Client Commands
Commands in this Section .......................... 1935
release dhcp ................................. 1936
renew dhcp ................................. 1936
show dhcp lease ............................ 1938

**DHCP Server Commands** .............................. 1940

Commands in this Section .......................... 1941
ip dhcp pool .................................... 1941
bootfile ......................................... 1944
clear ip dhcp binding ......................... 1944
clear ip dhcp conflict ......................... 1945
client-identifier .............................. 1946
client-name .................................... 1946
default-router .................................. 1947
dns-server (IP DHCP Pool Config) ............ 1948
domain-name (IP DHCP Pool Config) ......... 1949
hardware-address ............................... 1949
host .............................................. 1950
ip dhcp bootp automatic .................... 1951
ip dhcp conflict logging ..................... 1952
ip dhcp excluded-address .................... 1952
ip dhcp ping packets ......................... 1953
lease ................................. 1954
netbios-name-server ................. 1955
netbios-node-type ................... 1956
network ............................. 1957
next-server ........................... 1957
option ............................... 1958
service dhcp ........................ 1963
snmp .................................. 1963
show ip dhcp binding ................ 1964
show ip dhcp conflict ............... 1965
show ip dhcp global configuration .. 1965
show ip dhcp pool .................... 1966
show ip dhcp server statistics .... 1966
show ip dhcp server statistics .... 1966

DHCPv6 Server Commands ............... 1968

clear ipv6 dhcp ....................... 1968
dns-server (IPv6 DHCP Pool Config) . 1969
domain-name (IPv6 DHCP Pool Config) . 1969
ipv6 dhcp pool ....................... 1970
ipv6 dhcp relay ...................... 1971
ipv6 dhcp server .................... 1972
prefix-delegation .................... 1974
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>service dhcpv6</td>
<td>1975</td>
</tr>
<tr>
<td>show ipv6 dhcp</td>
<td>1976</td>
</tr>
<tr>
<td>show ipv6 dhcp binding.</td>
<td>1976</td>
</tr>
<tr>
<td>show ipv6 dhcp interface (User Exec)</td>
<td>1977</td>
</tr>
<tr>
<td>show ipv6 dhcp interface (Privileged Exec)</td>
<td>1978</td>
</tr>
<tr>
<td>show ipv6 dhcp pool</td>
<td>1981</td>
</tr>
<tr>
<td>show ipv6 dhcp statistics</td>
<td>1982</td>
</tr>
</tbody>
</table>

### HiveAgent Commands 1984

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands in this Section</td>
<td>1984</td>
</tr>
<tr>
<td>eula-consent</td>
<td>1984</td>
</tr>
<tr>
<td>hiveagent</td>
<td>1985</td>
</tr>
<tr>
<td>server</td>
<td>1986</td>
</tr>
<tr>
<td>debug</td>
<td>1987</td>
</tr>
<tr>
<td>enable</td>
<td>1988</td>
</tr>
<tr>
<td>proxy-ip-address</td>
<td>1989</td>
</tr>
<tr>
<td>source-interface vlan-id</td>
<td>1990</td>
</tr>
<tr>
<td>url</td>
<td>1991</td>
</tr>
<tr>
<td>show hiveagent debug</td>
<td>1992</td>
</tr>
<tr>
<td>show hiveagent source-interface</td>
<td>1992</td>
</tr>
<tr>
<td>show hiveagent status</td>
<td>1993</td>
</tr>
<tr>
<td>show eula-consent hiveagent</td>
<td>1994</td>
</tr>
</tbody>
</table>

### IP Addressing Commands 1996
Commands in this Section .......................... 1996

clear host ................................. 1997

clear ip address-conflict-detect .............. 1997

interface out-of-band ...................... 1998

ip address ................................. 1999

ip address (Out-of-Band) ............... 2001

ip address-conflict-detect run .......... 2002

ip address dhcp (Interface Configuration) .. 2003

ip default-gateway ...................... 2004

ip domain-lookup ......................... 2005

ip domain-name ......................... 2006

ip host .................................. 2007

ip name-server ........................ 2008

ip name-server source-interface ....... 2008

ipv6 address (Interface Configuration) ... 2010

ipv6 address (OOB Port) ................. 2012

ipv6 address dhcp ........................ 2013

ipv6 enable (Interface Configuration) .... 2014

ipv6 enable (OOB Configuration) ........ 2014

ipv6 gateway (OOB Configuration) ....... 2015

show hosts ................................ 2016
show ip address-conflict .................................. 2017
show ip helper-address ................................. 2018
show ipv6 dhcp interface out-of-band statistics  .... 2019
show ipv6 interface out-of-band ...................... 2020

Line Commands ........................................... 2022

accounting ............................................. 2022
authorization .......................................... 2023
enable authentication ................................. 2024
exec-banner ........................................... 2025
exec-timeout .......................................... 2026
history .................................................. 2027
history size ........................................... 2027
line ...................................................... 2028
login authentication .................................. 2029
login-banner .......................................... 2030
motd-banner .......................................... 2031
password (Line Configuration) ........................ 2031
show line .............................................. 2032
speed .................................................. 2033
terminal length ...................................... 2034

PHY Diagnostics Commands ......................... 2036
show copper-ports tdr .......................... 2036
show fiber-ports optical-transceiver ......... 2037
test copper-port tdr ............................ 2038

**Power Over Ethernet Commands .................. 2040**

Flexible Power Management .................. 2040

Commands in this Section .................... 2041

power inline .................................... 2041
power inline detection ......................... 2042
power inline four-pair forced ................. 2043
power inline limit ............................. 2044
power inline management ..................... 2046
power inline powered-device ................. 2048
power inline priority ......................... 2049
power inline reset ............................. 2049
power inline usage-threshold ................. 2050
clear power inline statistics ................. 2051
show power inline ............................ 2052

show power inline firmware-version .......... 2053

**RMON Commands ............................. 2055**

Commands in this Section .................... 2055

rmon alarm ..................................... 2055
rmon collection history ....................... 2057
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon event</td>
<td>2058</td>
</tr>
<tr>
<td>rmon hcalarm</td>
<td>2059</td>
</tr>
<tr>
<td>show rmon alarm</td>
<td>2061</td>
</tr>
<tr>
<td>show rmon alarms</td>
<td>2063</td>
</tr>
<tr>
<td>show rmon collection history</td>
<td>2064</td>
</tr>
<tr>
<td>show rmon events</td>
<td>2065</td>
</tr>
<tr>
<td>show rmon hcalarm</td>
<td>2066</td>
</tr>
<tr>
<td>show rmon history</td>
<td>2067</td>
</tr>
<tr>
<td>show rmon log</td>
<td>2070</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>2071</td>
</tr>
</tbody>
</table>

**Serviceability Commands** ........................................ 2075

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands in this Section</td>
<td>2075</td>
</tr>
<tr>
<td>debug aaa accounting</td>
<td>2076</td>
</tr>
<tr>
<td>debug arp</td>
<td>2077</td>
</tr>
<tr>
<td>debug authentication interface</td>
<td>2078</td>
</tr>
<tr>
<td>debug auto-voip</td>
<td>2079</td>
</tr>
<tr>
<td>debug bfd</td>
<td>2079</td>
</tr>
<tr>
<td>debug cfm</td>
<td>2080</td>
</tr>
<tr>
<td>debug clear</td>
<td>2081</td>
</tr>
<tr>
<td>debug console</td>
<td>2082</td>
</tr>
<tr>
<td>debug crashlog</td>
<td>2082</td>
</tr>
</tbody>
</table>
debug dhcp packet ........................... 2085

ddebug dhcp server packet .................... 2086

ddebug dot1ag ............................... 2087

ddebug dot1x ................................. 2088

ddebug igmpsnooping .......................... 2089

ddebug ip acl ................................. 2090

ddebug ip bgp ................................ 2090

ddebug ip dvmrp ............................... 2092

ddebug ip igmp ................................ 2093

ddebug ip mcache .............................. 2094

ddebug ip pimdm packet ...................... 2094

ddebug ip pimsms packet ..................... 2095

ddebug ipv6 dhcp ............................. 2096

ddebug ipv6 mcache ........................... 2097

ddebug ipv6 mld ............................... 2097

ddebug ipv6 pimdm ............................ 2098

ddebug ipv6 pimsms ............................ 2099

ddebug isdp .................................. 2100

ddebug lacp ................................... 2101

ddebug mldsnooping ........................... 2101

ddebug ospf .................................. 2102
debug ospfv3 .................................... 2103
debug ping ...................................... 2104
debug rip ........................................ 2105
debug sflow ................................. 2105
debug spanning-tree ....................... 2106
debug udld ..................................... 2107
debug vpc ....................................... 2108
debug vrrp ..................................... 2109
exception core-file .......................... 2109
exception dump ............................... 2110
exception protocol .......................... 2112
exception switch-chip-register ............ 2115
ip http timeout-policy ..................... 2115
show debugging .............................. 2116
show supported mibs ....................... 2119
snapshot bgp ................................. 2124
write core ..................................... 2125

Sflow Commands ................................ 2127

Commands in this Section ................... 2127
sflow destination ......................... 2127
sflow polling ............................... 2129
snmp-server enable traps ................................. 2153
snmp-server engineID local ............................... 2156
snmp-server filter ............................................. 2157
snmp-server group ............................................ 2159
snmp-server host .............................................. 2160
snmp-server location ...................................... 2162
snmp-server user .............................................. 2163
snmp-server view ............................................. 2165
snmp-server v3-host ......................................... 2166
snmp-server source-interface ......................... 2168

SupportAssist Commands ................................. 2170

Commands in this Section ................................. 2170
eula-consent ................................................. 2170
contact-company ............................................. 2172
contact-person ............................................... 2173
enable .......................................................... 2174
proxy-ip-address ............................................. 2175
server .......................................................... 2176
show eula-consent support-assist .................... 2177
show support-assist status ............................... 2179
support-assist ............................................... 2180
SYSLOG Commands

Command Logging

Commands in this Section

clear logging

clear logging file

description (Logging)

level

logging cli-command

logging
c
logging audit

logging buffered

logging console

logging facility

logging file

logging monitor

logging on

logging protocol

logging snmp

logging source-interface

logging traps
logging web-session .......................... 2202
port ............................................. 2203
show logging ................................. 2204
show logging file ............................ 2206
show syslog-servers ......................... 2206
terminal monitor ............................ 2207

**System and Stack Management Commands ........................ 2209**
asset-tag .................................... 2210
banner exec .................................. 2211
banner login .................................. 2211
banner motd .................................. 2212
banner motd acknowledge .................. 2213
buffers ........................................ 2215
clear checkpoint statistics ................ 2217
clear counters stack-ports ............... 2217
connect ....................................... 2218
cut-through mode. ......................... 2219
disconnect .................................. 2220
exit ............................................ 2221
hardware profile portmode .............. 2222
hostname ..................................... 2223
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiate failover</td>
<td>2224</td>
</tr>
<tr>
<td>load-interval</td>
<td>2225</td>
</tr>
<tr>
<td>locate</td>
<td>2226</td>
</tr>
<tr>
<td>logout</td>
<td>2227</td>
</tr>
<tr>
<td>member</td>
<td>2228</td>
</tr>
<tr>
<td>memory free low-watermark</td>
<td>2229</td>
</tr>
<tr>
<td>nsf</td>
<td>2230</td>
</tr>
<tr>
<td>ping</td>
<td>2230</td>
</tr>
<tr>
<td>process cpu threshold</td>
<td>2234</td>
</tr>
<tr>
<td>quit</td>
<td>2235</td>
</tr>
<tr>
<td>reload</td>
<td>2236</td>
</tr>
<tr>
<td>service unsupported-transceiver</td>
<td>2238</td>
</tr>
<tr>
<td>set description</td>
<td>2238</td>
</tr>
<tr>
<td>slot</td>
<td>2239</td>
</tr>
<tr>
<td>show banner</td>
<td>2241</td>
</tr>
<tr>
<td>show buffers</td>
<td>2242</td>
</tr>
<tr>
<td>show checkpoint statistics</td>
<td>2243</td>
</tr>
<tr>
<td>show cut-through mode</td>
<td>2244</td>
</tr>
<tr>
<td>show hardware profile</td>
<td>2244</td>
</tr>
<tr>
<td>show idprom interface</td>
<td>2245</td>
</tr>
<tr>
<td>show interfaces</td>
<td>2246</td>
</tr>
</tbody>
</table>
show interfaces advanced firmware .... 2248
show interfaces utilization .......... 2249
show memory cpu .................. 2252
show nsf ................................ 2253
show power-usage-history .......... 2255
show process app-list ............... 2256
show process app-resource-list .... 2258
show process cpu ................... 2259
show process proc-list ............. 2260
show router-capability ............. 2262
show sessions ........................ 2263
show slot ............................ 2264
show supported cardtype ........... 2266
show supported switchtype ......... 2268
show switch .......................... 2270
show system .......................... 2275
show system fan ..................... 2277
show system id ...................... 2278
show system power .................. 2278
show system temperature .......... 2279
show tech-support .................. 2281
show users ........................................ 2284
show version ..................................... 2285
stack ............................................. 2286
stack-port ....................................... 2287
stack-port shutdown ............................. 2289
standby .......................................... 2290
switch renumber ................................ 2291
telnet ............................................ 2292
traceroute ....................................... 2293
traceroute ipv6 ................................... 2296
update bootcode ................................ 2298

**Telnet Server Commands** .......................... 2299

Telnet Client Behaviors ......................... 2299

Commands in this Section ..................... 2301

ip telnet server disable ....................... 2301
ip telnet port .................................. 2302

show ip telnet .................................. 2302

**Time Ranges Commands** ....................... 2304

time-range [name] ............................. 2304

absolute ....................................... 2305

periodic ........................................ 2306

show time-range ............................... 2308
USB Flash Drive Commands ................. 2310

Validation of Files Downloaded/Uploaded from USB Device .......... 2310

Validation for Files Uploaded from Switch to USB Flash Drive .......... 2310

Downloading and Uploading of Files .......... 2311

Commands in this Section .......... 2311

unmount usb .......... 2311

show usb .......... 2312

dir usb. .......... 2313

recover .......... 2315

User Interface Commands ................. 2316

configure terminal .......... 2316

do .......... 2316

enable. .......... 2318

end .......... 2319

exit .......... 2320

quit .......... 2320

Web Server Commands ................. 2322

Web Sessions. .......... 2322

Commands in this Section .......... 2323

common-name .......... 2323
country ............................................. 2324
crypto certificate generate ..................... 2325
crypto certificate import ........................ 2327
crypto certificate request ....................... 2329
duration ............................................. 2330
ip http port ........................................ 2331
ip http server ...................................... 2332
ip http secure-certificate ....................... 2333
ip http secure-port ................................. 2333
ip http secure-server .............................. 2334
key-generate ...................................... 2335
location .............................................. 2336
no crypto certificate ............................... 2336
organization-unit ................................. 2337
show crypto certificate mycertificate .......... 2338
show ip http server status ...................... 2339
show ip http server secure status ............. 2340
state .................................................. 2341

A  Appendix A: List of Commands .............. 2343
Dell EMC Networking CLI

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Introduction

The Command Line Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, the user has greater configuration flexibility. The CLI is a basic command-line interpreter with command-line completion, in-line syntax help, and prior command recall.

A switch can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered by a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a console terminal connected to an RS-232 port or through a Telnet/SSH session. Serial communication via a dedicated USB port is available on the N1100-ON Series switch.

This guide describes how the CLI is structured, describes the command syntax, and describes the command functionality.

This guide also provides guidelines for configuring the Dell EMC Networking switch, and provides limited configuration examples. Basic installation is described in the User’s Guide and must be completed before using this document.

This document applies to the following switch firmware versions:

- Version 6.3.0.x—N2000, N3000, and N4000 Series switches
- Version 6.3.5.x—N3100-ON Series switches
- Version 6.3.6.x—N2100-ON, and N3100-ON Series switches
- Version 6.4.x.x—N1100-ON Series switches
## Command Groups

The system commands can be broken down into three sets of functional groups: Layer 2, Layer 3, and Utility.

### Table 1-1. System Command Groups

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layer 2 Commands</strong></td>
<td></td>
</tr>
<tr>
<td>ACL</td>
<td>Configures and displays ACL information.</td>
</tr>
<tr>
<td>MAC Address Table</td>
<td>Configures bridging address tables.</td>
</tr>
<tr>
<td>Auto-VoIP</td>
<td>Configures auto VoIP for IP phones on a switch.</td>
</tr>
<tr>
<td>CDP Interoperability</td>
<td>Configures Cisco® Discovery Protocol (CDP).</td>
</tr>
<tr>
<td>DHCP L2 Relay</td>
<td>Enables the Layer 2 DHCP relay agent for an interface.</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>Configures DHCP snooping and displays DHCP snooping information.</td>
</tr>
<tr>
<td>Dynamic ARP Inspection</td>
<td>Configures for rejection of invalid and malicious ARP packets.</td>
</tr>
<tr>
<td>Ethernet Configuration</td>
<td>Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.</td>
</tr>
<tr>
<td>Ethernet CFM</td>
<td>Configures and displays GVRP configuration and information.</td>
</tr>
<tr>
<td>Green Ethernet</td>
<td>Configures Green Ethernet and displays Green Ethernet information.</td>
</tr>
<tr>
<td>GVRP</td>
<td>Configures GVRP snooping and displays GVRP information.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Configures IGMP snooping and displays IGMP configuration and IGMP information.</td>
</tr>
<tr>
<td>IGMP Snooping Querier</td>
<td>Configures IGMP Snooping Querier and displays IGMP Snooping Querier information.</td>
</tr>
<tr>
<td>Interface Error Disable and Auto Recovery</td>
<td>Automatically disables an interface when an error is detected. Auto recovery re-enables the interface after the configured time interval expires.</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>Configures and manages IP addresses on the switch.</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 ACL</td>
<td>Configures and displays ACL information for IPv6.</td>
</tr>
<tr>
<td>IPv6 MLD Snooping</td>
<td>Configures IPv6 MLD Snooping.</td>
</tr>
<tr>
<td>IP Source Guard</td>
<td>Configures IP source guard and displays IP source guard information.</td>
</tr>
<tr>
<td>iSCSI Optimization</td>
<td>Configures special QoS treatment for traffic between iSCSI initiators and target systems.</td>
</tr>
<tr>
<td>Link Dependency</td>
<td>Configures and displays link dependency information.</td>
</tr>
<tr>
<td>LLDP</td>
<td>Configures and displays LLDP information.</td>
</tr>
<tr>
<td>Loop Protection</td>
<td>Configures keep alive.</td>
</tr>
<tr>
<td>MLAG</td>
<td>Configures MLAG and displays MLAG information.</td>
</tr>
<tr>
<td>Multicast VLAN Registration</td>
<td>Configures MVLAN and displays MVLAN information.</td>
</tr>
<tr>
<td>Port Channel</td>
<td>Configures and displays port channel information.</td>
</tr>
<tr>
<td>Port Monitor</td>
<td>Monitors activity on specific target ports.</td>
</tr>
<tr>
<td>QoS</td>
<td>Configures and displays QoS information.</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>Configures and reports on spanning tree protocol.</td>
</tr>
<tr>
<td>UDLD</td>
<td>Configures UDLD and displays UDLD information.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Configures VLANs and displays VLAN information.</td>
</tr>
<tr>
<td>Switchport Voice VLAN</td>
<td>Configures voice VLANs and displays voice VLAN information.</td>
</tr>
</tbody>
</table>

**Security Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Configures connection security including authorization and passwords.</td>
</tr>
<tr>
<td>Administrative Profiles</td>
<td>Group commands into a profile and assign a profile to a user upon authentication.</td>
</tr>
<tr>
<td>Commands</td>
<td></td>
</tr>
<tr>
<td>E-mail Alerting</td>
<td>Configures e-mail capabilities.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Configures and displays RADIUS information.</td>
</tr>
</tbody>
</table>
Table 1-1. System Command Groups (continued)

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+</td>
<td>Configures and displays TACACS+ information.</td>
</tr>
<tr>
<td>802.1x</td>
<td>Configures and displays commands related to 802.1x security protocol.</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Blocks clients from accessing network until user verification is established.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Provides several Denial of Service options.</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Configures and displays management access-list information.</td>
</tr>
<tr>
<td>Password Management</td>
<td>Provides password management.</td>
</tr>
<tr>
<td>SSH</td>
<td>Configures SSH authentication.</td>
</tr>
</tbody>
</table>

**Audio Visual Bridging Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMRP</td>
<td>Configures and displays MMRP information.</td>
</tr>
<tr>
<td>MSRP</td>
<td>Configures and displays MSRP information.</td>
</tr>
<tr>
<td>MVRP</td>
<td>Configures and displays MVRP information.</td>
</tr>
<tr>
<td>802.1AS Timesync</td>
<td>Configures and displays commands related to 802.1AS timesync.</td>
</tr>
</tbody>
</table>

**Data Center Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Bridging</td>
<td>Configures data center bridging snooping and displays data center bridging information.</td>
</tr>
<tr>
<td>OpenFlow</td>
<td>Configures the switch to be managed by a centralized OpenFlow Controller using the OpenFlow protocol.</td>
</tr>
<tr>
<td>Priority Flow Control</td>
<td>Configures priority flow control and displays priority flow control information.</td>
</tr>
</tbody>
</table>

**Layer 3 Routing Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP (IPv4)</td>
<td>Manages Address Resolution Protocol functions.</td>
</tr>
<tr>
<td>BFD</td>
<td>Configures BFD and displays BFD information.</td>
</tr>
<tr>
<td>BGP</td>
<td>Configures BGP and displays BGP information.</td>
</tr>
<tr>
<td>BGP Routing Policy</td>
<td>Configures BGP routing policy and displays BGP routing policy information.</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHCP Server and Relay Agent (IPv4)</td>
<td>Manages DHCP/BOOTP operations on the system.</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Configures IPv6 DHCP functions.</td>
</tr>
<tr>
<td>DHCPv6 Snooping</td>
<td>Configures DHCP v6 snooping and whether an interface is trusted or untrusted.</td>
</tr>
<tr>
<td>DVMRP (Mcast)</td>
<td>Configures DVMRP operations.</td>
</tr>
<tr>
<td>GMRP (Mcast)</td>
<td>Configures GMRP and displays GMRP information.</td>
</tr>
<tr>
<td>IGMP (Mcast)</td>
<td>Configures IGMP operations.</td>
</tr>
<tr>
<td>IGMP Proxy (Mcast)</td>
<td>Manages IGMP Proxy on the system.</td>
</tr>
<tr>
<td>IP Helper/DHCP Relay</td>
<td>Configures relay of UDP packets.</td>
</tr>
<tr>
<td>IP Routing (IPv4)</td>
<td>Configures IP routing and addressing.</td>
</tr>
<tr>
<td>IPv6 Multicast</td>
<td>Manages IPv6 multicasting on the system.</td>
</tr>
<tr>
<td>IPv6 Routing</td>
<td>Configures IPv6 routing and addressing.</td>
</tr>
<tr>
<td>Loopback Interface (IPv6)</td>
<td>Manages loopback configurations.</td>
</tr>
<tr>
<td>Multicast (Mcast)</td>
<td>Manages multicasting on the system.</td>
</tr>
<tr>
<td>OSPF (IPv4)</td>
<td>Manages shortest path operations.</td>
</tr>
<tr>
<td>OSPFv3 (IPv6)</td>
<td>Manages IPv6 shortest path operations.</td>
</tr>
<tr>
<td>Router Discovery Protocol (IPv4)</td>
<td>Manages router discovery operations.</td>
</tr>
<tr>
<td>Routing Information Protocol (IPv4)</td>
<td>Configures RIP activities.</td>
</tr>
<tr>
<td>Tunnel Interface (IPv6)</td>
<td>Managing tunneling operations.</td>
</tr>
<tr>
<td>Virtual Router</td>
<td>Manages a virtual router.</td>
</tr>
<tr>
<td>Virtual Router Redundancy (IPv4)</td>
<td>Controls virtual LAN routing.</td>
</tr>
</tbody>
</table>

**Switch Management Commands**

<p>| Application Deployment               | Manages Dell-supplied applications.                                        |</p>
<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Install</td>
<td>Automatically configures switch when a configuration file is not found.</td>
</tr>
<tr>
<td>CLI Macro</td>
<td>Configures CLI Macro and displays CLI Macro information.</td>
</tr>
<tr>
<td>Clock</td>
<td>Configures the system clock.</td>
</tr>
<tr>
<td>Command Line Configuration Scripting</td>
<td>Manages the switch configuration files.</td>
</tr>
<tr>
<td>Configuration and Image Files</td>
<td>Manages file system and Command Line Interface scripting commands.</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Configures an interface to obtain an IP address via DHCP.</td>
</tr>
<tr>
<td>HiveAgent</td>
<td>Enables configuration of the Dell HiveAgent</td>
</tr>
<tr>
<td>Line</td>
<td>Configures the console, SSH, and remote Telnet connection.</td>
</tr>
<tr>
<td>PHY Diagnostics</td>
<td>Diagnoses and displays the interface status.</td>
</tr>
<tr>
<td>Power Over Ethernet (PoE)</td>
<td>Configures PoE and displays PoE information.</td>
</tr>
<tr>
<td>RMON</td>
<td>Can be configured through the CLI and displays RMON information.</td>
</tr>
<tr>
<td>Serviceability Tracing</td>
<td>Controls display of debug output to serial port or telnet console.</td>
</tr>
<tr>
<td>sFlow</td>
<td>Configures sFlow monitoring.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Configures SNMP communities, traps and displays SNMP information.</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>Manages and displays SYSLOG messages.</td>
</tr>
<tr>
<td>System Management</td>
<td>Configures the switch clock, name and authorized users.</td>
</tr>
<tr>
<td>Telnet Server</td>
<td>Configures telnet service on the switch and displays telnet information.</td>
</tr>
<tr>
<td>Time Ranges</td>
<td>Configures time ranges and displays time range information.</td>
</tr>
<tr>
<td>USB Flash Drive</td>
<td>Configures USB flash drive and displays USB flash drive information.</td>
</tr>
</tbody>
</table>
Table 1-1. System Command Groups (continued)

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td>Describes user commands used for entering CLI commands.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Configures web-based access to the switch.</td>
</tr>
</tbody>
</table>

**Mode Types**

The tables on the following pages use these abbreviations for Command Mode names.

- AAA — IAS User Configuration
- APC — Administrative Profile Configuration
- ARPA — ARP ACL Configuration
- BR—BGP Router Configuration
- CC — Crypto Configuration
- CP — Captive Portal Configuration
- CPI — Captive Portal Instance
- CMC — Class-Map Configuration
- DCB—Datacenter-Bridging Configuration
- DP — IP DHCP Pool Configuration
- DRC—Dynamic RADIUS Configuration mode
- GC — Global Configuration
- HAC—Hive Agent Server Configuration
- IC — Interface Configuration
- IP — IP Access List Configuration
- IPAF4—IPv4 Address Family Configuration
- IPAF—IPv6 Address Family Configuration
- IR — Interface Range
- KC — Key Chain
- KE — Key
- L — Logging
- LC — Line Configuration
- LD — Link Dependency
- MA — Management Access-level
- MC — MST Configuration
- MD — MLAG Domain Configuration
- MDC — Maintenance Domain Configuration
- ML — MAC-List Configuration
- MSC — Mail Server Configuration
- MT — MAC-acl
- OFC — OpenFlow Configuration
- OG — OSPFv2 Global Configuration
- OR — OSPFv2 Router Configuration
- PE — Privileged Exec
- PM — Policy Map Configuration
- PCGC — Policy Map Global Configuration
- PCMC — Policy Class Map Configuration
- PTC — Peer Template Configuration
- R — RADIUS Server Configuration
- RIP — Router RIP Configuration
- RC — Router Configuration
- RM — Route Map Configuration
- ROSPF — Router Open Shortest Path First
- ROSV3 — Router Open Shortest Path First Version 3
- S — Support
- SAC — Support Assist Configuration
- SC — Stack Configuration
- SP — SSH Public Key
- SK — SSH Public Key-chain
• TC — TACACS Configuration
• TRC — Time Range Configuration
• UB—U-boot
• UE — User Exec
• VC — VLAN Configuration (reached via vlan command)
• VRC—VRF Configuration
• VR—Virtual Router Configuration
• v6ACL — IPv6 Access List Configuration
• v6CMC — IPv6 Class-Map Configuration
• v6DP — IPv6 DHCP Pool Configuration

**Layer 2 Commands**

**ACL**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list</td>
<td>Creates an Access Control List (ACL) that is identified by the parameter accesslistnumber.</td>
<td>GC</td>
</tr>
<tr>
<td>deny</td>
<td>permit (IP ACL)</td>
<td>The <strong>deny</strong> command denies traffic if the conditions defined in the deny statement are matched. The <strong>permit</strong> command allows traffic if the conditions defined in the permit statement are matched.</td>
</tr>
<tr>
<td>deny</td>
<td>permit (Mac-Access-List-Configuration)</td>
<td>The <strong>deny</strong> command denies traffic if the conditions defined in the deny statement are matched. The <strong>permit</strong> command allows traffic if the conditions defined in the permit statement are matched.</td>
</tr>
<tr>
<td>ip access-group</td>
<td>Attaches a specified access-control list to an interface.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>mac access-group</td>
<td>Attaches a specific MAC Access Control List (ACL) to an interface in the in-bound direction.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><code>mac access-list extended</code></td>
<td>Creates the MAC Access Control List (ACL) identified by the name parameter.</td>
<td>GC</td>
</tr>
<tr>
<td><code>mac access-list extended</code></td>
<td>Renames the existing MAC Access Control List (ACL) name.</td>
<td>GC</td>
</tr>
<tr>
<td><code>remark</code></td>
<td>Adds a comment to an ACL rule.</td>
<td>IPAF4, IPAF, ML, ARPA</td>
</tr>
<tr>
<td><code>service-acl input</code></td>
<td>Blocks Link Local Protocol Filtering (LLPF) protocol(s) on a given port.</td>
<td>IC</td>
</tr>
<tr>
<td><code>show access-lists interface</code></td>
<td>Displays interface ACLs.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show service-acl interface</code></td>
<td>Displays the status of LLPF rules configured on a particular port or on all the ports.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip access-lists</code></td>
<td>Displays an Access Control List (ACL) and all of the rules that are defined for the ACL.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show mac access-lists</code></td>
<td>Displays a MAC access list and all of the rules that are defined for the ACL.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

### MAC Address Table

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear mac address-table</code></td>
<td>Removes any learned entries from the forwarding database.</td>
<td>PE</td>
</tr>
<tr>
<td><code>mac address-table aging-time</code></td>
<td>Sets the address table aging time.</td>
<td>GC</td>
</tr>
<tr>
<td><code>mac address-table multicast forbidden address</code></td>
<td>Forbids adding a specific multicast address to specific ports.</td>
<td>GC</td>
</tr>
<tr>
<td><code>mac address-table static</code></td>
<td>Registers MAC-layer multicast addresses to the bridge forwarding table, and adds static ports to the group.</td>
<td>GC</td>
</tr>
<tr>
<td><code>switchport port-security (Interface Configuration)</code></td>
<td>Disables new address learning on an interface.</td>
<td>IC</td>
</tr>
</tbody>
</table>
| **Command** | **Description** | **Mode**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table</td>
<td>Displays dynamically created entries in the bridge-forwarding database.</td>
<td>PE</td>
</tr>
<tr>
<td>show mac address-table address</td>
<td>Displays all entries in the bridge-forwarding database for the specified MAC address.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show mac address-table count</td>
<td>Displays the number of addresses present in the Forwarding Database.</td>
<td>PE</td>
</tr>
<tr>
<td>show mac address-table dynamic</td>
<td>Displays all entries in the bridge-forwarding database.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show mac address-table interface</td>
<td>Displays the mac forwarding table entries for a specific interface.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show mac address-table multicast</td>
<td>Displays multicast MAC address table information.</td>
<td>PE</td>
</tr>
<tr>
<td>show mac address-table static</td>
<td>Displays statically created entries in the bridge-forwarding database.</td>
<td>PE</td>
</tr>
<tr>
<td>show mac address-table vlan</td>
<td>Displays all entries in the bridge-forwarding database for the specified VLAN.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show port-security</td>
<td>Displays the port-lock status.</td>
<td>PE</td>
</tr>
</tbody>
</table>

*a. For the meaning of each Mode abbreviation, see Mode Types.*

### Auto-VoIP

| **Command** | **Description** | **Mode**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport voice detect auto</td>
<td>Enables the VoIP Profile on all the interfaces of the switch.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>show switchport voice</td>
<td>Displays the status of auto-voip on an interface or all interfaces.</td>
<td>PE</td>
</tr>
</tbody>
</table>

*a. For the meaning of each Mode abbreviation, see Mode Types.*

### CDP Interoperability

| **Command** | **Description** | **Mode**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isdp counters</td>
<td>Clears the ISDP counters.</td>
<td>PE</td>
</tr>
<tr>
<td>clear isdp table</td>
<td>Clears entries in the ISDP table.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### DHCP L2 Relay

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp l2relay (Global Configuration)</td>
<td>Enables the Layer 2 DHCP Relay agent for an interface or globally.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>dhcp l2relay (Interface Configuration)</td>
<td>Enables DHCP L2 Relay for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>dhcp l2relay circuit-id</td>
<td>Enables user to set the DHCP Option 82 Circuit ID for a VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>dhcp l2relay remote-id</td>
<td>Enables user to set the DHCP Option 82 Remote ID for a VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>dhcp l2relay trust</td>
<td>Configures an interface to trust a received DHCP Option 82.</td>
<td>IC</td>
</tr>
<tr>
<td>dhcp l2relay vlan</td>
<td>Enables the L2 DHCP Relay agent for a set of VLANs.</td>
<td>GC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.
### DHCP Snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Modea</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip dhcp snooping binding</td>
<td>Clears all DHCP Snooping entries.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip dhcp snooping statistics</td>
<td>Clears all DHCP Snooping statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>ip dhcp snooping</td>
<td>Enables DHCP snooping globally or on a specific VLAN.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>ip dhcp snooping binding</td>
<td>Configures a static DHCP Snooping binding.</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping database</td>
<td>Configures the persistent location of the DHCP snooping database.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

For the meaning of each Mode abbreviation, see Mode Types.
### Dynamic ARP Inspection

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping database</td>
<td>Configures the interval in seconds at which the DHCP Snooping database will be stored in persistent storage.</td>
<td>GC</td>
</tr>
<tr>
<td>write-delay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip dhcp snooping limit</td>
<td>Controls the maximum rate of DHCP messages.</td>
<td>IC</td>
</tr>
<tr>
<td>ip dhcp snooping log-invalid</td>
<td>Enables logging of DHCP messages filtered by the DHCP Snooping application.</td>
<td>IC</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>Configure a port as trusted for DHCP snooping.</td>
<td>IC</td>
</tr>
<tr>
<td>ip dhcp snooping verify mac-address</td>
<td>Enables the verification of the source MAC address with the client MAC address in the received DHCP message.</td>
<td>GC</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping global and per port configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays the DHCP snooping binding entries.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping database</td>
<td>Displays the DHCP snooping configuration related to the database persistence.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping interfaces</td>
<td>Displays the DHCP Snooping status of the interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping statistics</td>
<td>Displays the DHCP snooping filtration statistics.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
### Ethernet Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp inspection limit</td>
<td>Configures the rate limit and burst interval values for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip arp inspection trust</td>
<td>Configures an interface as trusted for Dynamic ARP Inspection.</td>
<td>IC</td>
</tr>
<tr>
<td>ip arp inspection validate</td>
<td>Enables additional validation checks like source MAC address validation, destination MAC address validation or IP address validation on the received ARP packets.</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection vlan</td>
<td>Enables Dynamic ARP Inspection on a single VLAN or a range of VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>permit ip host mac host</td>
<td>Configures a rule for a valid IP address and MAC address combination used in ARP packet validation.</td>
<td>ARPA</td>
</tr>
<tr>
<td>show arp access-list</td>
<td>Displays the configured ARP ACLs with the rules.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Displays the Dynamic ARP Inspection configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>12 Enabled Disabled</td>
<td>Displays the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enters the interface configuration mode to configure parameters for an interface.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>interface range</td>
<td>Enters the interface configuration mode to execute a command on multiple ports at the same time.</td>
<td>GC or IC or IR</td>
</tr>
<tr>
<td>link debounce time</td>
<td>Configures the debounce timer for one or multiple interfaces.</td>
<td>IC or IR</td>
</tr>
<tr>
<td>rate-limit cpu</td>
<td>Reduces the amount of unknown unicast/multicast packets forwarded to the CPU.</td>
<td>GC</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Lists the traffic statistics for one or multiple interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces advertise</td>
<td>Displays information about auto negotiation advertisement.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces configuration</td>
<td>Displays the configuration for all configured interfaces.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces counters</td>
<td>Displays traffic seen by the Ethernet interface.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces debounce</td>
<td>Lists the debounce information for one or multiple interfaces.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show interfaces description</td>
<td>Displays the description for all configured interfaces.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces detail</td>
<td>Displays the detail for all configured interfaces.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the status for all configured interfaces.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces transceiver</td>
<td>Display the optic static parameters as well as the Dell EMC qualification.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces trunk</td>
<td>Display active trunk interface information.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays statistics for one port or for the entire switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show statistics switchport</td>
<td>Displays detailed statistics for a specific port or for the entire switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show storm-control</td>
<td>Displays the storm control configuration.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### Ethernet CFM

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm domain</td>
<td>Enters into maintenance domain Configuration mode for an existing domain. Use the optional level parameter to create a domain and enter into maintenance domain Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>service</td>
<td>Associates a VLAN with a maintenance domain.</td>
<td>MDC</td>
</tr>
<tr>
<td>ethernet cfm cc level</td>
<td>Initiates sending continuity checks (CCMs) at the specified interval and level on a VLAN monitored by an existing domain.</td>
<td>GC</td>
</tr>
<tr>
<td>ethernet cfm mep level</td>
<td>Creates a Maintenance End Point (MEP) on an interface at the specified level and direction.</td>
<td>IC</td>
</tr>
<tr>
<td>ethernet cfm mep enable</td>
<td>Enables a MEP at the specified level and direction.</td>
<td>IC</td>
</tr>
<tr>
<td>ethernet cfm mep active</td>
<td>Activates a MEP at the specified level and direction.</td>
<td>IC</td>
</tr>
<tr>
<td>ethernet cfm mep archive-hold-time</td>
<td>Maintains internal information on a missing MEP.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ethernet cfm mip level</td>
<td>Creates a Maintenance Intermediate Point (MIP) at the specified level.</td>
<td>IC</td>
</tr>
<tr>
<td>ping ethernet cfm</td>
<td>Generates a loopback message (LBM) from the configured MEP.</td>
<td>PE</td>
</tr>
<tr>
<td>traceroute ethernet cfm</td>
<td>Generates a link trace message (LTM) from the configured MEP.</td>
<td>PE</td>
</tr>
<tr>
<td>show ethernet cfm errors</td>
<td>Displays the cfm errors.</td>
<td>PE</td>
</tr>
<tr>
<td>show ethernet cfm domain</td>
<td>Displays the configured parameters in a maintenance domain.</td>
<td>PE</td>
</tr>
<tr>
<td>show ethernet cfm maintenance-points local</td>
<td>Displays the configured local maintenance points.</td>
<td>PE</td>
</tr>
<tr>
<td>show ethernet cfm maintenance-points remote</td>
<td>Displays the configured remote maintenance points.</td>
<td>PE</td>
</tr>
<tr>
<td>show ethernet cfm statistics</td>
<td>Displays the CFM statistics.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**Green Ethernet**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters</td>
<td>Enables a Dell EMC proprietary mode of power reduction on ports that are not connected to another interface.</td>
<td>IC</td>
</tr>
<tr>
<td>green-mode eee</td>
<td>Enables EEE low power idle mode on an interface or all the interfaces.</td>
<td>IC</td>
</tr>
<tr>
<td>description</td>
<td>Clears:</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>• The EEE LPI event count, and LPI duration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The EEE LPI history table entries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The Cumulative Power savings estimates for a specified interface or for all the interfaces based upon the argument.</td>
<td></td>
</tr>
<tr>
<td>green-mode eee-lpi-history</td>
<td>Configures the Global EEE LPI history collection interval and buffer size. This value is applied globally on all interfaces on the stack.</td>
<td>GC</td>
</tr>
</tbody>
</table>
### GVRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show green-mode interface-id</td>
<td>Displays the green-mode configuration and operational status of the port. This command is also used to display the per port configuration and operational status of the green-mode. The status is shown only for the modes supported on the corresponding hardware platform whether enabled or disabled.</td>
<td>PE</td>
</tr>
<tr>
<td>show green-mode</td>
<td>Displays the green-mode configuration for the whole system. The status is shown only for the modes supported on the corresponding hardware platform whether enabled or disabled.</td>
<td>PE</td>
</tr>
<tr>
<td>show green-mode eee-lpi-history interface</td>
<td>Displays the interface green-mode EEE LPI history.</td>
<td>PE</td>
</tr>
<tr>
<td>clear gvrp statistics</td>
<td>Clears all the GVRP statistics information.</td>
<td>PE</td>
</tr>
<tr>
<td>garp timer</td>
<td>Adjusts the GARP application join, leave, and leaveall GARP timer values.</td>
<td>IC</td>
</tr>
<tr>
<td>gvrp enable (Global Configuration)</td>
<td>Enables GVRP globally.</td>
<td>GC</td>
</tr>
<tr>
<td>gvrp enable (Interface Configuration)</td>
<td>Enables GVRP on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>gvrp registration-forbid</td>
<td>Deregisters all VLANs, and prevents dynamic VLAN registration on the port.</td>
<td>IC</td>
</tr>
<tr>
<td>gvrp vlan-creation-forbid</td>
<td>Enables or disables dynamic VLAN creation.</td>
<td>IC</td>
</tr>
<tr>
<td>show gvrp configuration</td>
<td>Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.</td>
<td>PE</td>
</tr>
<tr>
<td>show gvrp error-statistics</td>
<td>Displays GVRP error statistics.</td>
<td>UE</td>
</tr>
<tr>
<td>show gvrp statistics</td>
<td>Displays GVRP statistics.</td>
<td>UE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
a. For the meaning of each Mode abbreviation, see Mode Types.

### IGMP Snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping</code></td>
<td>In Global Configuration mode, Enables Internet Group Management Protocol (IGMP) snooping.</td>
<td>GC</td>
</tr>
<tr>
<td><code>show ip igmp snooping groups</code></td>
<td>Displays multicast groups learned by IGMP snooping.</td>
<td>UE</td>
</tr>
<tr>
<td><code>show ip igmp snooping mrouter</code></td>
<td>Displays information on dynamically learned multicast router interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip igmp snooping</code></td>
<td>In VLAN Configuration mode, enables IGMP snooping on a particular VLAN or on all interfaces participating in a VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan immediate-leave</code></td>
<td>Enables or disables IGMP Snooping fast-leave mode on a selected VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan groupmembership-interval</code></td>
<td>Sets the IGMP Group Membership Interval time on a VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan last-member-query-interval</code></td>
<td>Sets the IGMP Maximum Response time on a particular VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan mcrtrexpiretime</code></td>
<td>Sets the multicast router present expiration time.</td>
<td>VC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan report-suppression</code></td>
<td>Enables IGMP report suppression on a specific VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td><code>ip igmp snooping unregistered floodall</code></td>
<td>Enables flooding of unregistered multicast traffic to all ports in the VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan mrouter</code></td>
<td>Statically configures a port as connected to a multicast router for a specified VLAN.</td>
<td>GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
IGMP Snooping Querier

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Enables/disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN.</td>
<td>GC or VC</td>
</tr>
<tr>
<td>ip igmp snooping querier election participate</td>
<td>Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td>ip igmp snooping querier query-interval</td>
<td>Sets the IGMP Querier Query Interval time.</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping querier timer expiry</td>
<td>Sets the IGMP Querier timer expiration period.</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping querier version</td>
<td>Sets the IGMP version of the query that the snooping switch is going to send periodically.</td>
<td>GC</td>
</tr>
<tr>
<td>show ip igmp snooping querier</td>
<td>Displays IGMP Snooping Querier information.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

Interface Error Disable and Auto Recovery

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable recovery cause</td>
<td>Enables automatic recovery of any interface when disabled from the listed cause</td>
<td>GC</td>
</tr>
<tr>
<td>errdisable recovery interval</td>
<td>Configures the interval for error recovery of interfaces disabled due to any cause.</td>
<td>GC</td>
</tr>
<tr>
<td>show errdisable recovery</td>
<td>Displays the error disable configuration for each possible cause.</td>
<td>GC</td>
</tr>
<tr>
<td>show interfaces status err-disabled</td>
<td>Displays the interfaces that are error disabled by the system.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
### IP Addressing

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear host</td>
<td>Deletes entries from the host name-to-address cache.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip address-conflict-detect</td>
<td>Clears the address conflict detection status in the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>interface out-of-band</td>
<td>Enters into OOB interface configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>ip address</td>
<td>Configures an IP address on an in-band interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip address (Out-of-Band)</td>
<td>Sets an IP address for the out-of-band interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip address-conflict-detect run</td>
<td>Triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>ip address dhcp (Interface Configuration)</td>
<td>Acquires an IP address on an interface from the DHCP server.</td>
<td>IC</td>
</tr>
<tr>
<td>ip default-gateway</td>
<td>Defines a default gateway (router).</td>
<td>GC</td>
</tr>
<tr>
<td>ip domain-lookup</td>
<td>Enables IP DNS-based host name-to-address translation.</td>
<td>GC</td>
</tr>
<tr>
<td>ip domain-name</td>
<td>Defines a default domain name to complete unqualified host names.</td>
<td>GC</td>
</tr>
<tr>
<td>ip host</td>
<td>Configures static host name-to-address mapping in the host cache.</td>
<td>GC</td>
</tr>
<tr>
<td>ip name-server</td>
<td>Defines available IPv4 or IPv6 name servers.</td>
<td>GC</td>
</tr>
<tr>
<td>ip name-server source-interface</td>
<td>Configures available name servers.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 address (Interface Configuration)</td>
<td>Sets the IPv6 address of the management interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 address (OOB Port)</td>
<td>Sets the IPv6 prefix on the out-of-band port.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 address dhcp</td>
<td>Enables the DHCPv6 client on an IPv6 interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 enable (Interface Configuration)</td>
<td>Enables IPv6 on the management interface.</td>
<td>GC</td>
</tr>
</tbody>
</table>
### IPv6 ACL

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a new rule for the current IPv6 access list.</td>
<td>v6ACL</td>
</tr>
<tr>
<td>permit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>Creates an IPv6 Access Control List (ACL) consisting of classification fields defined for the IP header of an IPv6 frame.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 access-list rename</td>
<td>Changes the name of an IPv6 ACL.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 traffic-filter</td>
<td>Attaches a specific IPv6 ACL to an interface or associates it with a VLAN ID in a given direction.</td>
<td>GC</td>
</tr>
<tr>
<td>show ipv6 access-lists</td>
<td>Displays an IPv6 access list (and the rules defined for it).</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

**IPv6 ACL**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 enable (OOB Configuration)</td>
<td>Enables IPv6 operation on the out-of-band interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 gateway (OOB Configuration)</td>
<td>Configures the address of the IPv6 gateway.</td>
<td>IC</td>
</tr>
<tr>
<td>show hosts</td>
<td>Displays the default domain name, a list of name server hosts, static and cached list of host names and addresses.</td>
<td>UE</td>
</tr>
<tr>
<td>show ip address-conflict</td>
<td>Displays the status information corresponding to the last detected address conflict.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip helper-address</td>
<td>Displays the ip helper addresses configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 dhcp interface out-of-band statistics</td>
<td>Displays IPv6 DHCP statistics for the out-of-band interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 interface out-of-band</td>
<td>Displays the IPv6 out-of-band port configuration.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

### Table of Commands and Descriptions

- **Command**
- **Description**
- **Mode**

---

a. For the meaning of each Mode abbreviation, see [Mode Types](#).
## IPv6 MLD Snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping vlan groupmembership-interval</td>
<td>Sets the MLD Group Membership Interval time on a VLAN or interface.</td>
<td>VC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan immediate-leave</td>
<td>Enables or disables MLD Snooping immediate-leave admin mode on a selected interface or VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan last-listener-query-interval</td>
<td>Sets the MLD Maximum Response time for an interface or VLAN.</td>
<td>IC or VC</td>
</tr>
<tr>
<td>ipv6 mld snooping listener-message-suppression</td>
<td>Enables MLD listener message suppression on a specific VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan mcrtexpiretime</td>
<td>Sets the multicast router present expiration time.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan mrouter</td>
<td>Statically configures a port as connected to a multicast router for a specified VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping (Global)</td>
<td>Enables MLD Snooping on the system (Global Configuration mode).</td>
<td>GC</td>
</tr>
<tr>
<td>show ipv6 mld snooping</td>
<td>Displays MLD snooping information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping groups</td>
<td>Displays the MLD snooping entries in the MFDB table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>Displays information on dynamically learned multicast router interfaces.</td>
<td>PE</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

## IPv6 MLD Snooping Querier

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping querier</td>
<td>Enables MLD Snooping Querier on the system.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping querier (VLAN mode)</td>
<td>Enables MLD Snooping Querier on a VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td>ipv6 mld snooping querier address</td>
<td>Sets the global MLD Snooping Querier address on the system or on a VLAN.</td>
<td>GC or VC</td>
</tr>
</tbody>
</table>
### IP Source Guard

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify source</code></td>
<td>Enables IP Source Guard on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td><code>ip verify binding</code></td>
<td>Configures IPSG static bindings.</td>
<td>GC</td>
</tr>
<tr>
<td><code>show ip verify</code></td>
<td>Displays IPSG interface configuration.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip verify source</code></td>
<td>Displays the bindings configured on a particular interface.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip source binding</code></td>
<td>Displays all bindings (static and dynamic).</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a. For the meaning of each Mode abbreviation, see Mode Types.

### iSCSI Optimization

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>iscsi cos</code></td>
<td>Sets the quality of service profile that will be applied to iSCSI flows.</td>
<td>GC</td>
</tr>
<tr>
<td><code>iscsi enable</code></td>
<td>Enables Global Configuration mode command globally enables iSCSI awareness.</td>
<td>GC</td>
</tr>
<tr>
<td><code>show iscsi</code></td>
<td>Displays the iSCSI settings.</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a. For the meaning of each Mode abbreviation, see Mode Types.
Link Dependency

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Indicates if the link-dependency group should mirror or invert the status of the depended on interfaces.</td>
<td>LD</td>
</tr>
<tr>
<td>link-dependency group</td>
<td>Enters the link-dependency mode to configure a link-dependency group.</td>
<td>GC</td>
</tr>
<tr>
<td>add</td>
<td>Adds member gigabit Ethernet port(s) to the dependency list.</td>
<td>LD</td>
</tr>
<tr>
<td>depends-on</td>
<td>Adds the dependent Ethernet ports or port channels list.</td>
<td>LD</td>
</tr>
<tr>
<td>show link-dependency</td>
<td>Shows the link dependencies configured on a particular group.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

LLDP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lldp remote-data</td>
<td>Deletes all data from the remote data table.</td>
<td>PE</td>
</tr>
<tr>
<td>clear lldp statistics</td>
<td>Resets all LLDP statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>dcb enable</td>
<td>Enables the sending of DCBX information in LLDP frames.</td>
<td>GC</td>
</tr>
<tr>
<td>debug lldp</td>
<td>Displays LLDP debug information.</td>
<td>PE</td>
</tr>
<tr>
<td>lldp med</td>
<td>Enables/disables LLDP-MED on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med configuraton</td>
<td>Enables sending the topology change notification.</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med faststartrepeatcount</td>
<td>Sets the value of the fast start repeat count.</td>
<td>GC</td>
</tr>
<tr>
<td>lldp med transmit-tlv</td>
<td>Specifies which optional TLVs in the LLDP MED set are transmitted in the LLDPDUs.</td>
<td>IC</td>
</tr>
<tr>
<td>lldp notification</td>
<td>Enables remote data change notifications.</td>
<td>IC</td>
</tr>
<tr>
<td>lldp notification-interval</td>
<td>Limits how frequently remote data change notifications are sent.</td>
<td>GC</td>
</tr>
</tbody>
</table>
Loop Protection

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive (Interface Config)</td>
<td>Enables loop protection on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>keepalive (Global Config)</td>
<td>Globally enable loop protection and optionally configure the loop protection timer and packet count.</td>
<td>GC</td>
</tr>
<tr>
<td>keepalive action</td>
<td>Configure the action taken when a loop is detected on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show keepalive</td>
<td>Displays the global loop protect configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show keepalive statistics</td>
<td>Displays the loop protect status for one or all interfaces.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

## MLAG

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear vpc statistics</td>
<td>Clears the counters for the keepalive messages transmitted and received by the MLAG switch.</td>
<td>PE</td>
</tr>
<tr>
<td>feature vpc</td>
<td>Enables debug traces for the specified protocols.</td>
<td>GC</td>
</tr>
<tr>
<td>feature vpc</td>
<td>Globally enables MLAG.</td>
<td>GC</td>
</tr>
<tr>
<td>peer detection enable</td>
<td>Enables the Dual Control Plane Detection Protocol.</td>
<td>MD</td>
</tr>
<tr>
<td>peer detection interval</td>
<td>Configures the peer detection transmission interval and the detection interval.</td>
<td>MD</td>
</tr>
<tr>
<td>peer-keepalive destination</td>
<td>Enables the Dual Control Plane Detection Protocol with the configured IP address of the peer MLAG, the local source address and the peer timeout value.</td>
<td>MD</td>
</tr>
<tr>
<td>peer-keepalive enable</td>
<td>Enables the peer keepalive protocol.</td>
<td>MD</td>
</tr>
<tr>
<td>peer-keepalive timeout</td>
<td>Configures the peer keepalive timeout value, in seconds.</td>
<td>MD</td>
</tr>
<tr>
<td>role priority</td>
<td>Configures the priority value used on a switch for primary/secondary role selection.</td>
<td>MD</td>
</tr>
<tr>
<td>show vpc</td>
<td>Displays information about an MLAG.</td>
<td>PE</td>
</tr>
<tr>
<td>show vpc brief</td>
<td>Displays the MLAG global status.</td>
<td>PE</td>
</tr>
</tbody>
</table>
## Multicast VLAN Registration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvr</td>
<td>Enables MVR.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>mvr group</td>
<td>Adds an MVR membership group.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vpc consistency-parameters</td>
<td>Displays MLAG-related configuration information in a format suitable for comparison with the other MLAG peer.</td>
<td>PE</td>
</tr>
<tr>
<td>show vpc consistency-features</td>
<td>Displays MLAG-related configuration information in a format suitable for comparison with the other MLAG peer.</td>
<td>PE</td>
</tr>
<tr>
<td>show vpc peer-keepalive</td>
<td>Displays the peer MLAG switch’s IP address used by the dual control plane detection protocol.</td>
<td>PE</td>
</tr>
<tr>
<td>show vpc role</td>
<td>Displays information about the keepalive status, keepalive parameters, role of the MLAG switch, and the system MAC and priority.</td>
<td>PE</td>
</tr>
<tr>
<td>show vpc statistics</td>
<td>Displays counters for the keepalive messages transmitted and received by the MLAG switch</td>
<td>PE</td>
</tr>
<tr>
<td>system-mac</td>
<td>Manually configures the MAC address for the VPC domain.</td>
<td>MD</td>
</tr>
<tr>
<td>system-priority</td>
<td>Manually configures the priority for the VPC domain.</td>
<td>MD</td>
</tr>
<tr>
<td>vpc</td>
<td>Configures a port-channel (LAG) as part of the MLAG domain.</td>
<td>IC</td>
</tr>
<tr>
<td>vpc domain</td>
<td>Enters into MLAG Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>vpc peer-link</td>
<td>Configures a port channel as the MLAG peer link for a domain and enables the peer link protocol.</td>
<td>IC</td>
</tr>
</tbody>
</table>

---

*a.* For the meaning of each Mode abbreviation, see **Mode Types**.

**Mode Types**

- **MC**: Management Console
- **MD**: Management Domain
- **PE**: Peer
- **IC**: Inter-Chassis
- **GC**: Inter-System

---

**Multicast VLAN Registration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvr</td>
<td>Enables MVR.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>mvr group</td>
<td>Adds an MVR membership group.</td>
<td>GC</td>
</tr>
</tbody>
</table>
### Port Channel

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group</td>
<td>Associates a port with a port-channel.</td>
<td>IC</td>
</tr>
<tr>
<td>feature vpc</td>
<td>Enables debug traces for the specified protocols.</td>
<td>GC</td>
</tr>
<tr>
<td>interface range port-channel</td>
<td>Enters the interface configuration mode to configure multiple port-channels.</td>
<td>GC</td>
</tr>
<tr>
<td>hashing-mode</td>
<td>Sets the hashing algorithm on trunk ports.</td>
<td>IC (port-channel)</td>
</tr>
<tr>
<td>lACP port-priority</td>
<td>Configures the priority value for Ethernet ports.</td>
<td>IC</td>
</tr>
<tr>
<td>lACP system-priority</td>
<td>Configures the system LACP priority.</td>
<td>GC</td>
</tr>
<tr>
<td>lACP timeout</td>
<td>Assigns an administrative LACP timeout.</td>
<td>IC</td>
</tr>
<tr>
<td>port-channel min-links</td>
<td>Sets the minimum number of links that must be up in order for the port channel interface to be declared up.</td>
<td>IC</td>
</tr>
</tbody>
</table>
Port Monitor

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture (Global Configuration)</td>
<td>Captures packets transmitted or received from the CPU.</td>
<td>GC</td>
</tr>
<tr>
<td>monitor capture (Privileged Exec)</td>
<td>Capture packets transmitted or received from the CPU</td>
<td>PE</td>
</tr>
<tr>
<td>monitor session</td>
<td>Configures a port monitoring session.</td>
<td>GC</td>
</tr>
<tr>
<td>remote-span</td>
<td>Configures a VLAN as an RSPAN VLAN.</td>
<td>VC</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays captured packets transmitted or received from the CPU.</td>
<td>PE</td>
</tr>
<tr>
<td>show monitor session</td>
<td>Displays the port monitoring status.</td>
<td>PE</td>
</tr>
<tr>
<td>show vlan remote-span</td>
<td>Displays the RSPAN VLAN IDs.</td>
<td>UE or PE</td>
</tr>
</tbody>
</table>

QoS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>assign-queue</td>
<td>Modifies the queue ID to which the associated traffic stream is assigned.</td>
<td>PCMC</td>
</tr>
<tr>
<td>class</td>
<td>Creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.</td>
<td>PMC</td>
</tr>
<tr>
<td>class-map</td>
<td>Defines a new DiffServ class of type match-all.</td>
<td>GC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>class-map rename</td>
<td>Changes the name of a DiffServ class.</td>
<td>GC</td>
</tr>
<tr>
<td>classofservice dot1p-mapping</td>
<td>Maps an 802.1p priority to an internal traffic class for a switch.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>classofservice ip-dscp-mapping</td>
<td>Maps an IP DSCP value to an internal traffic class.</td>
<td>GC</td>
</tr>
<tr>
<td>classofservice trust</td>
<td>Sets the class of service trust mode of an interface.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>conform-color</td>
<td>Specifies the precoloring of packets conforming to or exceeding the specified rate(s). The possible actions are drop, setdscp-transmit, set-prec-transmit, or transmit.</td>
<td>PCMC</td>
</tr>
<tr>
<td>cos-queue min-bandwidth</td>
<td>Specifies the minimum transmission bandwidth for each interface queue.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>cos-queue random-detect</td>
<td>Configures WRED packet drop policy on an interface CoS queue.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>cos-queue strict</td>
<td>Activates the strict priority scheduler mode for each specified queue.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>diffserv</td>
<td>Sets the DiffServ operational mode to active.</td>
<td>GC</td>
</tr>
<tr>
<td>drop</td>
<td>Use the <strong>drop policy-class-map configuration</strong> command to specify that all packets for the associated traffic stream are to be dropped at ingress.</td>
<td>PCMC</td>
</tr>
<tr>
<td>mark cos</td>
<td>Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header.</td>
<td>PCMC</td>
</tr>
<tr>
<td>mark ip-dscp</td>
<td>Marks all packets for the associated traffic stream with the specified IP DSCP value.</td>
<td>PCMC</td>
</tr>
<tr>
<td>mark ip-precedence</td>
<td>Marks all packets for the associated traffic stream with the specified IP precedence value.</td>
<td>PCMC</td>
</tr>
<tr>
<td>match access-group</td>
<td>Adds ACL match criteria to a class map.</td>
<td>CMC</td>
</tr>
<tr>
<td>match class-map</td>
<td>Adds add to the specified class definition the set of match conditions defined for another class.</td>
<td>CMC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>match cos</td>
<td>Adds to the specified class definition a match condition for the Class of Service value.</td>
<td>CMC</td>
</tr>
<tr>
<td>match destination-address mac</td>
<td>Adds to the specified class definition a match condition based on the destination MAC address of a packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match any</td>
<td>Allows matching on any of the specified match conditions.</td>
<td>CMC</td>
</tr>
<tr>
<td>match dstip</td>
<td>Adds to the specified class definition a match condition based on the destination IP address of a packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match dstip6</td>
<td>Adds to the specified class definition a match condition based on the destination IPv6 address of a packet.</td>
<td>v6CMC</td>
</tr>
<tr>
<td>match dstl4port</td>
<td>Adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword, or a numeric notation.</td>
<td>CMC</td>
</tr>
<tr>
<td>match ethertype</td>
<td>Adds to the specified class definition a match condition based on the value of the ethertype.</td>
<td>CMC</td>
</tr>
<tr>
<td>match ip6flowlbl</td>
<td>Adds to the specified class definition a match condition based on the IPv6 flow label of a packet.</td>
<td>v6CMC</td>
</tr>
<tr>
<td>match ip dscp</td>
<td>Adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match ip precedence</td>
<td>Adds to the specified class definition a match condition based on the value of the IP.</td>
<td>CMC</td>
</tr>
<tr>
<td>match ip tos</td>
<td>Adds to the specified class definition a match condition based on the value of the IP TOS field in a packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match protocol</td>
<td>Adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.</td>
<td>CMC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>match source-address mac</td>
<td>Adds to the specified class definition a match condition based on the source MAC address of the packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match srcip</td>
<td>Adds to the specified class definition a match condition based on the source IP address of a packet.</td>
<td>CMC</td>
</tr>
<tr>
<td>match srcip6</td>
<td>Adds to the specified class definition a match condition based on the source IPv6 address of a packet.</td>
<td>v6CMC</td>
</tr>
<tr>
<td>match srcL4port</td>
<td>Adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword, a numeric notation, or a numeric range notation.</td>
<td>CMC</td>
</tr>
<tr>
<td>match vlan</td>
<td>Adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field.</td>
<td>CMC</td>
</tr>
<tr>
<td>mirror</td>
<td>Mirrors all the data that matches the class defined to the destination port specified.</td>
<td>PCMC</td>
</tr>
<tr>
<td>police-simple</td>
<td>Implements simple color aware marking for the specified class.</td>
<td>PCMC</td>
</tr>
<tr>
<td>police-single-rate</td>
<td>Implements a single-rate Three Color Marker (trTCM) per RFC 2698</td>
<td>PCMC</td>
</tr>
<tr>
<td>police-two-rate</td>
<td>Implements a two-rate Three Color Marker (trTCM) per RFC 2698.</td>
<td>PCMC</td>
</tr>
<tr>
<td>policy-map</td>
<td>Establishes a new DiffServ policy or enters policy map configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>random-detect queue-params</td>
<td>Configures the green, yellow and red TCP and non-TCP packet minimum and maximum thresholds and corresponding drop probabilities on an interface or all interfaces.</td>
<td>GC, IC, or IR</td>
</tr>
<tr>
<td>random-detect exponential-weighting-constant</td>
<td>Configures the decay in the calculation of the average queue size user for WRED on an interface or all interfaces.</td>
<td>GC, IC, or IR</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode²</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>redirect</td>
<td>Specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (Ethernet port or port-channel).</td>
<td>PCMC</td>
</tr>
<tr>
<td>service-policy</td>
<td>Attaches a policy to an interface in a particular direction.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>show class-map</td>
<td>Displays all configuration information for the specified class.</td>
<td>PE</td>
</tr>
<tr>
<td>show classofservice dot1p-mapping</td>
<td>Displays the current 802.1p priority mapping to internal traffic classes for a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show classofservice ip-dscp-mapping</td>
<td>Displays the current IP DSCP mapping to internal traffic classes for a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show classofservice trust</td>
<td>Displays the current trust mode setting for a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show diffserv</td>
<td>Displays the DiffServ General Status information.</td>
<td>PE</td>
</tr>
<tr>
<td>show diffserv service interface</td>
<td>Displays policy service information for the specified interface and direction.</td>
<td>PE</td>
</tr>
<tr>
<td>show diffserv service brief</td>
<td>Displays all interfaces in the system to which a DiffServ policy has been attached.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces cos-queue</td>
<td>Displays the class-of-service queue configuration for the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces random-detect</td>
<td>Displays the WRED policy on an interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays all configuration information for the specified policy.</td>
<td>PE</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays policy-oriented statistics information for the specified interface and direction.</td>
<td>PE</td>
</tr>
<tr>
<td>show service-policy</td>
<td>Displays a summary of policy-oriented statistics information for all interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>traffic-shape</td>
<td>Specifies the maximum transmission bandwidth limit for the interface as a whole.</td>
<td>GC or IC</td>
</tr>
</tbody>
</table>
### Spanning Tree

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan priority</code></td>
<td>Assigns a default VLAN priority tag for untagged frames ingressing an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>clear spanning-tree</td>
<td>Restarts the protocol migration process on all interfaces or on the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>detected-protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit (mst)</td>
<td>Exits the MST configuration mode and applies configuration changes.</td>
<td>MC</td>
</tr>
<tr>
<td>instance (mst)</td>
<td>Maps VLANs to an MST instance.</td>
<td>MG</td>
</tr>
<tr>
<td>name (MST)</td>
<td>Defines the MST configuration name.</td>
<td>MC</td>
</tr>
<tr>
<td>revision (mst)</td>
<td>Defines the configuration revision number.</td>
<td>MC</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>Displays spanning tree configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>summary</td>
<td>Displays spanning tree settings and parameters for the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show spanning-tree vlan</td>
<td>Displays spanning tree information per VLAN and also lists the port roles and states as well as the port cost.</td>
<td>PE</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables spanning-tree functionality.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree auto-portfast</td>
<td>Sets the port to auto portfast mode.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree backbonefast</td>
<td>Enables the detection of indirect link failures and accelerate spanning tree convergence on STP-PV/RSTP-PV configured switches using Indirect Link Rapid Convergence (IRC).</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree bpdu flooding</td>
<td>Allows flooding of BPDUs received on nonspanning-tree ports to all other non-spanning-tree ports.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree bpduprotection</td>
<td>Enables BPDUs protection on a switch.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree cost</td>
<td>Configures the spanning tree path cost for a port.</td>
<td>IC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree disable</td>
<td>Disables spanning tree on a specific port.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree forward-time</td>
<td>Configures the spanning tree bridge forward time.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree guard</td>
<td>Selects whether loop guard or root guard is enabled on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree loopguard</td>
<td>Enables loop guard on all ports.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree max-age</td>
<td>Configures the spanning tree bridge maximum age.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree max-hops</td>
<td>Sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree mode</td>
<td>Configures the spanning tree protocol.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree mst configuration</td>
<td>Enables configuring an MST region by entering the multiple spanning-tree (MST) mode.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree mst cost</td>
<td>Configures the path cost for multiple spanning tree (MST) calculations.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree mst port-priority</td>
<td>Configures port priority.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree mst priority</td>
<td>Configures the switch priority for the specified spanning tree instance.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree portfast</td>
<td>Enables portfast mode.</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree portfast bpdufilter default</td>
<td>Discards BPDUs received on spanningtree ports in portfast mode.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree portfast default</td>
<td>Enables portfast mode on all ports.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree port-priority</td>
<td>Configures port priority.</td>
<td>IC</td>
</tr>
<tr>
<td>(Interface Configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>spanning-tree priority</td>
<td>Configures the spanning tree priority.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree tcnguard</td>
<td>Prevents a port from propagating topology change notifications.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode⁴</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>spanning-tree transmit hold-count</td>
<td>Set the maximum number of BPDUs that a bridge is allowed to send within a hello time window (2 seconds).</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree uplinkfast</td>
<td>Configures the rate at which gratuitous frames are sent after a switchover to an alternate port and enables Direct Link Rapid Convergence.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan</td>
<td>Enables per VLAN spanning tree on a VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan forward-time</td>
<td>Configures the spanning tree forward delay time for a specified VLAN or a range of VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan hello-time</td>
<td>Configures the spanning tree hello time for a specified VLAN or a range of VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan max-age</td>
<td>Configures the spanning tree maximum age time for a set of VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan root</td>
<td>Configures the switch to become the root bridge or standby root bridge.</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree vlan priority</td>
<td>Configures the bridge priority of a VLAN.</td>
<td>GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**UDLD**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td>udld enable (Global Configuration)</td>
<td>Globally enable UDLD. UDLD must be globally enabled and enabled on an interface to operate.</td>
<td>GC</td>
</tr>
<tr>
<td>udld reset</td>
<td>Resets (enable) all interfaces disabled by UDLD.</td>
<td>PE</td>
</tr>
<tr>
<td>udld message time</td>
<td>Configures the interval between the transmission of UDLD probe messages on ports that are in the advertisement phase.</td>
<td>GC</td>
</tr>
<tr>
<td>udld timeout interval</td>
<td>Configures the interval for the receipt of ECHO replies.</td>
<td>GC</td>
</tr>
<tr>
<td>udld enable (Interface Configuration)</td>
<td>Enables UDLD on a specific interface.</td>
<td>IC</td>
</tr>
</tbody>
</table>
### VLAN

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>udld port</td>
<td>Selects the UDLD operating mode on a specific interface.</td>
<td>IC</td>
</tr>
<tr>
<td>show udld</td>
<td>Displays the global settings for UDLD.</td>
<td>PE</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see *Mode Types*.

### VLAN

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan</td>
<td>Enters the VLAN interface configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>interface range vlan</td>
<td>Enters the interface configuration mode to configure multiple VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>name (VLAN Configuration)</td>
<td>Configures a name to a VLAN.</td>
<td>IC</td>
</tr>
<tr>
<td>private-vlan</td>
<td>Defines a private VLAN association between the primary and secondary VLANs.</td>
<td>VC</td>
</tr>
<tr>
<td>protocol group</td>
<td>Attaches a vlan-id to the protocol-based VLAN identified by groupid.</td>
<td>VC</td>
</tr>
<tr>
<td>protocol vlan group</td>
<td>Adds the Ethernet interface to the protocol-based VLAN identified by groupid.</td>
<td>IC</td>
</tr>
<tr>
<td>protocol vlan group all</td>
<td>Adds all Ethernet interfaces to the protocol-based VLAN identified by groupid.</td>
<td>GC</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>Displays the QinQ status for each interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays switchport configuration.</td>
<td>PE or IC</td>
</tr>
<tr>
<td>show port protocol</td>
<td>Displays the Protocol-Based VLAN information for either the entire system or for the indicated group.</td>
<td>PE</td>
</tr>
<tr>
<td>show switchport ethertype</td>
<td>Displays the configured Ethertype for each interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays detailed information, including interface information and dynamic vlan type, for a specific VLAN.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show vlan association mac</td>
<td>Displays the VLAN associated with a specific configured MAC address.</td>
<td>PE</td>
</tr>
<tr>
<td>show vlan association subnet</td>
<td>Displays the VLAN associated with a specific configured IP subnet.</td>
<td>PE</td>
</tr>
<tr>
<td>show vlan private-vlan</td>
<td>Displays information about the configured private VLANs.</td>
<td>PE</td>
</tr>
<tr>
<td>switchport access vlan</td>
<td>Configures the PVID VLAN ID when the interface is in access mode.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport dot1q ethertype (Global Configuration)</td>
<td>Defines additional QinQ tunneling TPIDs for matching in the outer VLAN tag of received frames.</td>
<td>GC</td>
</tr>
<tr>
<td>switchport general forbidden vlan</td>
<td>Forbids adding specific VLANs to a port.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport general acceptable-frame-type tagged-only</td>
<td>Discards untagged frames at ingress.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport general allowed vlan</td>
<td>Adds or removes VLANs from a port in General mode.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport general ingress-filtering disable</td>
<td>Disables port ingress filtering.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport general pvid</td>
<td>Configures the PVID when the interface is in general mode.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport mode</td>
<td>Configures the VLAN membership mode of a port.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport mode private-vlan</td>
<td>Defines a private VLAN association for an isolated or community interface or a mapping for a promiscuous interface.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport mode dot1q-tunnel</td>
<td>Enables QinQ tunneling on customer edge (CE) interfaces.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport private-vlan</td>
<td>Defines a private VLAN association for an isolated or community port or a mapping for a promiscuous port.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport trunk</td>
<td>Adds or removes VLANs from a trunk port.</td>
<td>IC</td>
</tr>
</tbody>
</table>
### Switchport Voice VLAN

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport voice vlan</td>
<td>Enables the voice VLAN capability on the switch.</td>
<td>GG</td>
</tr>
<tr>
<td>switchport voice vlan (Interface)</td>
<td>Assigns the voice VLAN ID on the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan priority</td>
<td>Trusts or not trusts the data traffic arriving on the voice VLAN port.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan dot1p</td>
<td>Configure voice VLAN 802.1p priority tagging for voice traffic.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan dscp</td>
<td>Configure dscp value for voice traffic on the voice VLAN port.</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan none</td>
<td>Allow the IP phone to use its own configuration to send untagged voice traffic.</td>
<td>IC</td>
</tr>
</tbody>
</table>

---

a. For the meaning of each Mode abbreviation, see Mode Types.
### Security Commands

#### AAA

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting</td>
<td>Creates an accounting method list</td>
<td>GC</td>
</tr>
<tr>
<td>aaa accounting delay-start</td>
<td>Delays the sending of Acct-Start packets to RADIUS accounting server(s)</td>
<td>GC</td>
</tr>
<tr>
<td>aaa accounting update</td>
<td>Enables the sending of interim accounting packets to RADIUS accounting server(s).</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authentication dot1x default</td>
<td>Specifies an authentication method for 802.1x clients.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authentication enable</td>
<td>Defines authentication method lists for accessing higher privilege levels.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>Defines login authentication.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authorization</td>
<td>Creates an authorization method list.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authorization network default radius</td>
<td>Enables the switch to accept VLAN assignment by the RADIUS server.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa ias-user username</td>
<td>Configures IAS users and their attributes. Also changes the mode to aa user Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>This command is a no-op command. It is present only for compatibility purposes.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

*a. For the meaning of each Mode abbreviation, see [Mode Types](#).*
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa server radius dynamic-author</td>
<td>Enters radius dynamic authorization mode.</td>
<td>GC</td>
</tr>
<tr>
<td>authentication enable</td>
<td>Globally enables the Authentication Manager.</td>
<td>GC</td>
</tr>
<tr>
<td>authentication order</td>
<td>Sets the order of authentication methods used on a port.</td>
<td>IC</td>
</tr>
<tr>
<td>authentication priority</td>
<td>Sets the priority for the authentication methods used on a port.</td>
<td>IC</td>
</tr>
<tr>
<td>authentication restart</td>
<td>Sets the interval after which reauthentication starts.</td>
<td>IC</td>
</tr>
<tr>
<td>clear (IAS)</td>
<td>Deletes all IAS users.</td>
<td>PE</td>
</tr>
<tr>
<td>clear authentication statistics</td>
<td>Clears the authentication statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>clear authentication authentication-history</td>
<td>Clears the authentication history logs.</td>
<td>PE</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to the normal level.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http authentication</td>
<td>Specifies authentication methods for http.</td>
<td>GC</td>
</tr>
<tr>
<td>ip https authentication</td>
<td>Specifies authentication methods for https.</td>
<td>GC</td>
</tr>
<tr>
<td>password (AAA IAS User Configuration)</td>
<td>Configures a password for a user.</td>
<td>AAA</td>
</tr>
<tr>
<td>password (User Exec)</td>
<td>Specifies a user password</td>
<td>UE</td>
</tr>
<tr>
<td>show aaa ias-users</td>
<td>Displays configured IAS users and their attributes.</td>
<td>PE</td>
</tr>
<tr>
<td>show aaa statistics</td>
<td>Displays accounting statistics</td>
<td>PE</td>
</tr>
<tr>
<td>show accounting methods</td>
<td>Displays the configured accounting method lists.</td>
<td>PE</td>
</tr>
<tr>
<td>show authentication</td>
<td>Shows information about authentication methods.</td>
<td>PE</td>
</tr>
<tr>
<td>show authentication authentication-history</td>
<td>Displays the authentication history on one or more interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show authentication methods</td>
<td>Displays information about the authentication methods.</td>
<td>PE</td>
</tr>
</tbody>
</table>
## Administrative Profiles

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication statistics</td>
<td>Displays the Authentication Manager statistics on one or more interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show authorization methods</td>
<td>Displays the configured authorization method lists.</td>
<td>PE</td>
</tr>
<tr>
<td>show users accounts</td>
<td>Displays information about the local user database.</td>
<td>PE</td>
</tr>
<tr>
<td>show users login-history</td>
<td>Displays information about login histories of users.</td>
<td>PE</td>
</tr>
<tr>
<td>username</td>
<td>Establishes a username-based authentication system. Optionally allows the specification of an Administrative Profile for a local user.</td>
<td>GC</td>
</tr>
<tr>
<td>username unlock</td>
<td>Transfers local user passwords between devices without having to know the passwords.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

<sup>a</sup> For the meaning of each Mode abbreviation, see [Mode Types](#).

---

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-profile</td>
<td>Creates an administrative profile.</td>
<td>GC</td>
</tr>
<tr>
<td>description (Administrative Profile Configuration)</td>
<td>Adds a description to an administrative profile.</td>
<td>APC</td>
</tr>
<tr>
<td>rule</td>
<td>Adds a rule to an administrative profile.</td>
<td>APC</td>
</tr>
<tr>
<td>show admin-profiles</td>
<td>Displays the administrative profiles.</td>
<td>PE</td>
</tr>
<tr>
<td>show admin-profiles brief</td>
<td>Lists the names of the administrative profiles defined on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show cli modes</td>
<td>Lists the names of all the CLI modes.</td>
<td>PE</td>
</tr>
<tr>
<td>show users</td>
<td>Shows which administrative profiles have been assigned to local user accounts and to show which profiles are active for logged-in users.</td>
<td>PE</td>
</tr>
<tr>
<td>username</td>
<td>Optionally allows the specification of an Administrative Profile for a local user.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

<sup>a</sup> For the meaning of each Mode abbreviation, see [Mode Types](#).
### E-mail Alerting

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging email</td>
<td>Enables e-mail alerting and sets the lowest severity level for which log messages are e-mailed.</td>
<td>GC</td>
</tr>
<tr>
<td>logging email urgent</td>
<td>Sets the lowest severity level at which log messages are e-mailed in an urgent manner.</td>
<td>GC</td>
</tr>
<tr>
<td>logging email message-type</td>
<td>Sets the lowest severity level at which SNMP traps are logged.</td>
<td>GC</td>
</tr>
<tr>
<td>to-addr</td>
<td>Configures the To address field of the e-mail.</td>
<td>GC</td>
</tr>
<tr>
<td>logging email message-type</td>
<td>Configures the subject.</td>
<td>GC</td>
</tr>
<tr>
<td>to-addr</td>
<td>Configures the value of how frequently the queued messages are sent.</td>
<td>GC</td>
</tr>
<tr>
<td>logging email from-addr</td>
<td>Configures the From address of the e-mail.</td>
<td>GC</td>
</tr>
<tr>
<td>logging email message-type</td>
<td>Tests whether or not an e-mail is being sent to an SMTP server.</td>
<td>GC</td>
</tr>
<tr>
<td>subject</td>
<td>Displays information on how many e-mails are sent, how many e-mails failed, when the last e-mail was sent, how long it has been since the last e-mail was sent, how long it has been since the e-mail changed to disabled mode.</td>
<td>PE</td>
</tr>
<tr>
<td>clear logging email statistics</td>
<td>Clears the e-mail alerting statistics.</td>
<td>GC</td>
</tr>
<tr>
<td>security</td>
<td>Sets the e-mail alerting security protocol.</td>
<td>MSC</td>
</tr>
<tr>
<td>mail-server ip-address</td>
<td>Configures the SMTP server IP address and changes the mode to Mail Server Configuration Mode.</td>
<td>GC</td>
</tr>
<tr>
<td>hostname</td>
<td>Configures the TCP port to use for communication with the SMTP servers.</td>
<td>MSC</td>
</tr>
<tr>
<td>port (Mail Server Configuration Mode)</td>
<td>Configures the username required by the authentication.</td>
<td>MSC</td>
</tr>
<tr>
<td>username (Mail Server Configuration Mode)</td>
<td>Configures the password required to authenticate to the e-mail server.</td>
<td>MSC</td>
</tr>
<tr>
<td>password (Mail Server Configuration Mode)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### RADIUS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mail-server</td>
<td>Displays the configuration of all the mail servers or a particular mail server.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>acct-port</td>
<td>Sets the port that connects to the RADIUS accounting server.</td>
<td>R</td>
</tr>
<tr>
<td>attribute 6</td>
<td>Configures processing of the RADIUS Service-Type attribute.</td>
<td>R</td>
</tr>
<tr>
<td>attribute 8</td>
<td>Configures the switch to send the RADIUS Framed-IP-Address attribute in the Access-Request message sent to a specific RADIUS authentication server.</td>
<td>R</td>
</tr>
<tr>
<td>attribute 25</td>
<td>Enables the switch to send the RADIUS Class attribute as supplied by the RADIUS server in accounting messages sent to the specific accounting server.</td>
<td>R</td>
</tr>
<tr>
<td>attribute 31</td>
<td>Alters the format of the MAC address sent in the Calling-Station-Id attribute to the RADIUS server when authenticating using 802.1X MAC based authentication for an interface.</td>
<td>R</td>
</tr>
<tr>
<td>attribute 168 include-in-access-req</td>
<td>Enables the switch to send the RADIUS Framed-IPv6-Address attribute in accounting messages sent to the RADIUS accounting server.</td>
<td>R</td>
</tr>
<tr>
<td>authentication event fail retry</td>
<td>Sets the number of times authentication may be reattempted by the user for the RADIUS method for an IEEE 802.1X supplicant.</td>
<td>GC</td>
</tr>
<tr>
<td>auth-port</td>
<td>Sets the port number for authentication requests of the designated radius server.</td>
<td>R</td>
</tr>
<tr>
<td>automate-tester</td>
<td>Configures liveness checking.</td>
<td>R</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>deadtime</td>
<td>Improves RADIUS response times when a server is unavailable by causing the unavailable server to be skipped.</td>
<td>R</td>
</tr>
<tr>
<td>key</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.</td>
<td>R</td>
</tr>
<tr>
<td>msgauth</td>
<td>Enables the message authenticator attribute to be used for the RADIUS Authenticating server being configured.</td>
<td>R</td>
</tr>
<tr>
<td>name (RADIUS Server)</td>
<td>Assigns a list name to a RADIUS server</td>
<td>R</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies that a configured server should be the primary server in the group of authentication servers which have the same server name.</td>
<td>R</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the order in which the servers are to be used, with 0 being the highest priority.</td>
<td>R</td>
</tr>
<tr>
<td>radius server attribute 4</td>
<td>Sets the network access server (NAS) IP address for the RADIUS server.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server attribute 6</td>
<td>Enables the switch to send the RADIUS Service-Type attribute in authentication messages sent to the authentication server.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server attribute 8</td>
<td>Enables the switch to send the RADIUS Framed-IP-Address attribute in authentication messages sent to the authentication server.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server attribute 25</td>
<td>Globally enables the switch to send the RADIUS Class attribute as supplied by the RADIUS server in accounting messages sent to the accounting server.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server attribute 31</td>
<td>Globally enables the switch to send the RADIUS Class attribute as supplied by the RADIUS server in accounting messages sent to the accounting server.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server attribute 168</td>
<td>Enables the switch to send the RADIUS Framed-IPv6-Address attribute in accounting messages sent to the RADIUS accounting server.</td>
<td>GC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode³</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>radius server deadtime</td>
<td>Improves RADIUS response times when servers are unavailable. Causes the unavailable servers to be skipped.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server</td>
<td>Specifies a RADIUS server host.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server key</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server retransmit</td>
<td>Specifies the number of times the software searches the list of RADIUS server hosts.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server source-ip</td>
<td>Specifies the source IP address used for communication with RADIUS servers.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server source-interface</td>
<td>Selects the interface from which to use the IP address in the source IP address field of transmitted RADIUS packets.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server timeout</td>
<td>Sets the interval for which a switch waits for a RADIUS server to reply.</td>
<td>GC</td>
</tr>
<tr>
<td>radius server vsa send</td>
<td>Enables the switch to process during authentication.</td>
<td>GC</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>retransmit</td>
<td>Specifies the number of times the software searches the list of RADIUS server hosts before stopping the search.</td>
<td>R</td>
</tr>
<tr>
<td>show aaa servers</td>
<td>Displays the list of configured RADIUS servers and the values configured for the global parameters of the RADIUS client.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show radius statistics</td>
<td>Shows the statistics for an authentication or accounting server.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>source-ip</td>
<td>Specifies the source IP address to be used for communication with RADIUS servers.</td>
<td>R</td>
</tr>
<tr>
<td>timeout</td>
<td>Sets the timeout value in seconds for the designated RADIUS server.</td>
<td>R</td>
</tr>
<tr>
<td>usage</td>
<td>Specifies the usage type of the server.</td>
<td>R</td>
</tr>
</tbody>
</table>

³ For the meaning of each Mode abbreviation, see Mode Types.
### TACACS+

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server.</td>
<td>TC</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a server port number.</td>
<td>TC</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the order in which servers are used.</td>
<td>TC</td>
</tr>
<tr>
<td>show tacacs</td>
<td>Displays TACACS+ server settings and statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>tacacs-server host</td>
<td>Specifies a TACACS+ server host.</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon.</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server source-interface</td>
<td>Selects the interface from which to use the IP address in the source IP address field of transmitted TACACS packets.</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server timeout</td>
<td>Sets the interval for which the switch waits for a server host to reply.</td>
<td>GC</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout value in seconds.</td>
<td>TC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

### 802.1x

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x dynamic-vlan enable</td>
<td>Enables the capability of creating VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>dot1x eapolflood</td>
<td>Enables the flooding of received IEEE 802.1x frames in the VLAN.</td>
<td>GC</td>
</tr>
<tr>
<td>dot1x initialize</td>
<td>Begins the initialization sequence on the specified port.</td>
<td>PE</td>
</tr>
<tr>
<td>mab</td>
<td>Enables MAB on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>default mab</td>
<td>Configures the switch to transmit EAP, PAP, or CHAP credentials to the RADIUS server for MAB-authenticated devices connected to the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>mab request format</td>
<td>Configures the format of the MAC address sent in the User-Name attribute.</td>
<td>IC, GC</td>
</tr>
<tr>
<td>dot1x max-reauth-req</td>
<td>Sets the maximum number of times that the switch sends Extensible Authentication Protocol EAP-Request/Identity frames to which no response is received before restarting the authentication process.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times the switch sends an EAP-request frame to the client before restarting the authentication process.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x max-users</td>
<td>Sets the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>Enables manual control of the authorization state of the port.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>Manually initiates a reauthentication of all 802.1x-enabled ports or a specified 802.1X enabled port.</td>
<td>PE</td>
</tr>
<tr>
<td>dot1x reauthentication</td>
<td>Enables periodic reauthentication of the client.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x system-auth-control monitor</td>
<td>Enables 802.1X globally.</td>
<td>GC</td>
</tr>
<tr>
<td>dot1x timeout guest-vlan-period</td>
<td>Sets the number of seconds that the switch waits before authorizing the client if the client is a dot1x unaware client.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x timeout quiet-period</td>
<td>Sets the number of seconds the switch remains in the quiet state following a failed authentication attempt.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x timeout re-authperiod</td>
<td>Sets the number of seconds between reauthentication attempts.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>dot1x timeout server-timeout</td>
<td>Sets the number of seconds the switch waits for a response from the authentication server before resending the request.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x timeout supp-timeout</td>
<td>Sets the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x timeout tx-period</td>
<td>Sets the number of seconds the switch waits for a response to an EAP-request/identify frame from the client before resending the request.</td>
<td>IC</td>
</tr>
<tr>
<td>auth-type</td>
<td>Set the accepted authorization types for dynamic RADIUS clients.</td>
<td>DRC</td>
</tr>
<tr>
<td>client</td>
<td>Sets the CoA client parameters.</td>
<td>DRC</td>
</tr>
<tr>
<td>ignore</td>
<td>Sets the switch to ignore certain authentication parameters from dynamic RADIUS clients.</td>
<td>DRC</td>
</tr>
<tr>
<td>port</td>
<td>Sets the port on which to listen for CoA and disconnect requests from authorized dynamic RADIUS clients.</td>
<td>DRC</td>
</tr>
<tr>
<td>server-key</td>
<td>Configures a global shared secret that is used for all dynamic RADIUS clients that do not have an individual shared secret configured.</td>
<td>DRC</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays 802.1X status for the switch or the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show dot1x authentication-history</td>
<td>Displays the dot1x authentication events and information during successful and unsuccessful dot1x authentication processes.</td>
<td>PE</td>
</tr>
<tr>
<td>show dot1x clients</td>
<td>Displays detailed information about the users who have successfully authenticated on the system or on a specified port.</td>
<td>PE</td>
</tr>
<tr>
<td>show dot1x interface</td>
<td>Shows the status of MAC Authentication Bypass.</td>
<td>PE</td>
</tr>
<tr>
<td>show dot1x interface statistics</td>
<td>Displays 802.1X statistics for the specified interface.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### Dell EMC Networking CLI

#### Captive Portal

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x users</td>
<td>Displays active 802.1X authenticated users for the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>clear dot1x authentication-history</td>
<td>Clears the authentication history table captured during successful and unsuccessful authentication.</td>
<td>PE</td>
</tr>
<tr>
<td>dot1x guest-vlan</td>
<td>Sets the guest VLAN on a port.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x unauth-vlan</td>
<td>Specifies the unauthenticated VLAN on a port.</td>
<td>IC</td>
</tr>
<tr>
<td>show dot1x advanced</td>
<td>Displays 802.1X advanced features for the switch or specified interface.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

---

#### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication timeout</td>
<td>Configures the authentication timeout.</td>
<td>CP</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Enables the captive portal configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>enable</td>
<td>Globally enables captive portal.</td>
<td>CPI</td>
</tr>
<tr>
<td>http port</td>
<td>Configures an additional HTTP port for captive portal to monitor.</td>
<td>CP</td>
</tr>
<tr>
<td>https port</td>
<td>Configures an additional HTTPS port for captive portal to monitor.</td>
<td>CP</td>
</tr>
<tr>
<td>show captive-portal</td>
<td>Displays the status of captive portal.</td>
<td>PE</td>
</tr>
<tr>
<td>show captive-portal status</td>
<td>Reports the status of all captive portal instances in the system.</td>
<td>PE</td>
</tr>
<tr>
<td>block</td>
<td>Blocks all traffic for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>configuration</td>
<td>Enables the captive portal instance mode.</td>
<td>CP</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>group</td>
<td>Configures the group number for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>interface</td>
<td>Associates an interface with a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>locale</td>
<td>Associates an interface with a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>name (Captive Portal)</td>
<td>Configures the name for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>protocol</td>
<td>Configures the protocol mode for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>redirect</td>
<td>Enables the redirect mode for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>redirect-url</td>
<td>Configures the redirect URL for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>session-timeout</td>
<td>Configures the session timeout for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>verification</td>
<td>Configures the verification mode for a captive portal configuration.</td>
<td>CPI</td>
</tr>
<tr>
<td>captive-portal client deauthenticate</td>
<td>De-authenticates a specific captive portal client.</td>
<td>PE</td>
</tr>
<tr>
<td>show captive-portal client status</td>
<td>Displays client connection details or a connection summary for connected captive portal users.</td>
<td>PE</td>
</tr>
<tr>
<td>show captive-portal configuration client status</td>
<td>Displays the clients authenticated to all captive portal configurations or a to specific configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show captive-portal interface client status</td>
<td>Displays information about clients authenticated on all interfaces or a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show captive-portal interface configuration status</td>
<td>Displays the clients authenticated to all captive portal configurations or a to specific configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>clear captive-portal users</td>
<td>Deletes all captive portal user entries.</td>
<td>PE</td>
</tr>
<tr>
<td>no user</td>
<td>Deletes a user from the local user database.</td>
<td>CP</td>
</tr>
<tr>
<td>show captive-portal user</td>
<td>Displays all configured users or a specific user in the captive portal local user database.</td>
<td>PE</td>
</tr>
<tr>
<td>user group</td>
<td>Associates a group with a captive portal user.</td>
<td>CP</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>user-logout</td>
<td>Enables captive portal users to log out of the portal.</td>
<td>CPI</td>
</tr>
<tr>
<td>user name</td>
<td>Modifies the user name for a local captive portal user.</td>
<td>CP</td>
</tr>
<tr>
<td>user password</td>
<td>Creates a local user or changes the password for an existing user.</td>
<td>CP</td>
</tr>
<tr>
<td>user session-timeout</td>
<td>Sets the session timeout value for a captive portal user.</td>
<td>CP</td>
</tr>
<tr>
<td>show captive-portal</td>
<td>Displays the operational status of each captive portal configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show captive-portal</td>
<td>Displays information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>configuration interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show captive-portal</td>
<td>Displays locales associated with a specific captive portal configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>configuration locales</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show captive-portal</td>
<td>Displays information about all configured captive portal configurations or a specific captive portal configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>configuration status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user group</td>
<td>Creates a user group.</td>
<td>CP</td>
</tr>
<tr>
<td>user group moveusers</td>
<td>Moves a group's users to a different group.</td>
<td>CP</td>
</tr>
<tr>
<td>user group name</td>
<td>Configures a group name.</td>
<td>CP</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

### Denial of Service

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos-control</td>
<td>Enables Minimum TCP Header Size Denial of Service protection.</td>
<td>GC</td>
</tr>
<tr>
<td>firstfrag</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dos-control</td>
<td>Enables Maximum ICMP Packet Size Denial of Service protections.</td>
<td>GC</td>
</tr>
<tr>
<td>icmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dos-control</td>
<td>Enables L4 Port Denial of Service protection.</td>
<td>GC</td>
</tr>
<tr>
<td>l4port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Management ACL

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Modea</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny (management)</td>
<td>Defines a deny rule.</td>
<td>MA</td>
</tr>
<tr>
<td>management access-class</td>
<td>Defines which management access-list is used.</td>
<td>GC</td>
</tr>
<tr>
<td>management access-list</td>
<td>Defines a management access-list, and enters the access-list for configuration.</td>
<td>GC</td>
</tr>
<tr>
<td>no priority (management)</td>
<td>Removes a permit or deny condition from a Management Access list.</td>
<td>MA</td>
</tr>
<tr>
<td>permit (management)</td>
<td>Defines a permit rule.</td>
<td>MA</td>
</tr>
<tr>
<td>show management access-class</td>
<td>Displays the active management access-list.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Modea</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos-control sipdip</td>
<td>Enables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection.</td>
<td>GC</td>
</tr>
<tr>
<td>dos-control tcpflag</td>
<td>Enables TCP Flag Denial of Service protections.</td>
<td>GC</td>
</tr>
<tr>
<td>dos-control tcpfrag</td>
<td>Enables TCP Fragment Denial of Service protection.</td>
<td>GC</td>
</tr>
<tr>
<td>rate-limit cpu</td>
<td>Configures the rate in packets-per-second for the number of IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved hardware address of the destined IPv6 node.</td>
<td>GC</td>
</tr>
<tr>
<td>show dos-control</td>
<td>Displays Denial of Service configuration information.</td>
<td>PE</td>
</tr>
<tr>
<td>show system internal pktmgr</td>
<td>Displays the configured CPU rate limit for unknown packets in packets per second.</td>
<td>PE</td>
</tr>
<tr>
<td>storm-control broadcast</td>
<td>Enables Broadcast storm control.</td>
<td>IC</td>
</tr>
<tr>
<td>storm-control multicast</td>
<td>Enables the switch to count multicast packets together with broadcast packets.</td>
<td>IC</td>
</tr>
<tr>
<td>storm-control unicast</td>
<td>Enables unicast storm control.</td>
<td>IC</td>
</tr>
</tbody>
</table>

---
a. For the meaning of each Mode abbreviation, see Mode Types.
### Password Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>show management access-list</td>
<td>Displays management access-lists.</td>
<td>PE</td>
</tr>
<tr>
<td>passwords aging</td>
<td>Implements aging on the passwords such that users are required to change passwords when they expire.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords history</td>
<td>Enables the administrator to set the number of previous passwords that are stored to ensure that users do not reuse their passwords too frequently.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords lock-out</td>
<td>Enables the administrator to strengthen the security of the switch by enabling the user lockout feature. When a lockout count is configured, a user who is logging in must enter the correct password within that count.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords min-length</td>
<td>Enables the administrator to enforce a minimum length required for a password.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength-check</td>
<td>Enables the Password Strength feature.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength minimum upper-case-letters</td>
<td>Enforces a minimum number of uppercase letters that a password should contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength minimum lower-case-letters</td>
<td>Enforces a minimum number of lowercase letters that a password must contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength minimum numeric-characters</td>
<td>Enforces a minimum number of numeric numbers that a password should contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength minimum special-characters</td>
<td>Enforces a minimum number of special characters that a password may contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength max-limit consecutive-characters</td>
<td>Enforces a maximum number of consecutive characters that a password can contain.</td>
<td>GC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see [Mode Types](#).

---

**Note:** The table above provides a concise list of commands and their descriptions for managing passwords in a networking environment. Each command is designed to help administrators enforce and maintain secure password policies, ensuring that the network remains protected from unauthorized access.

---

**Dell EMC Networking CLI**

---

**Page 152**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwords strength max-limit repeated-characters</td>
<td>Enforces a maximum repeated characters that a password should contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength minimum character-classes</td>
<td>Enforces the minimum number of character classes (uppercase letters, lowercase letters, numeric characters and special characters) that a password must contain.</td>
<td>GC</td>
</tr>
<tr>
<td>passwords strength exclude-keyword</td>
<td>Enforces a maximum number of consecutive characters that a password can contain.</td>
<td>GC</td>
</tr>
<tr>
<td>enable password encrypted</td>
<td>Used by an Administrator to transfer the enable password between devices without having to know the password.</td>
<td>PE</td>
</tr>
<tr>
<td>show passwords configuration</td>
<td>Displays the configuration parameters for password configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show passwords result</td>
<td>Displays the last password set result information.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**SSH**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate dsa</td>
<td>Generates DSA key pairs for the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs for the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto key pubkey-chain ssh</td>
<td>Enters SSH Public Key-chain configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto key zeroize pubkey-chain</td>
<td>Erases all public key chains or the public key chain for a user.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto key zeroize {rsa</td>
<td>dsa}</td>
<td>Deletes the RSA or DSA keys from the switch.</td>
</tr>
<tr>
<td>ip ssh port</td>
<td>Specifies the port to be used by the SSH server.</td>
<td>GC</td>
</tr>
<tr>
<td>ip ssh pubkey-auth</td>
<td>Enables public key authentication for incoming SSH sessions.</td>
<td>GC</td>
</tr>
<tr>
<td>ip ssh server</td>
<td>Enables the switch to be configured from a SSH server connection.</td>
<td>GC</td>
</tr>
<tr>
<td>key-string</td>
<td>Manually specifies a SSH public key.</td>
<td>SK</td>
</tr>
</tbody>
</table>
show crypto key mypubkey  Displays its own SSH public keys stored on the switch.  PE

show crypto key pubkey-chain ssh  Displays SSH public keys stored on the switch.  PE

show ip ssh  Displays the SSH server configuration.  PE

a. For the meaning of each Mode abbreviation, see Mode Types.

Audio Visual Bridging Commands

MMRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode\textsuperscript{a}</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mmrp statistics</td>
<td>Clears the MMRP statistics for an interface or all interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>mmrp</td>
<td>Enables MMRP on a specific interface.</td>
<td>IC or IR</td>
</tr>
<tr>
<td>mmrp global</td>
<td>Globally enables MMRP.</td>
<td>GC</td>
</tr>
<tr>
<td>mmrp periodic state machine</td>
<td>Globally enables the MMRP periodic state machine.</td>
<td>GC</td>
</tr>
<tr>
<td>show mmrp</td>
<td>Displays the MMRP configuration for an interface or globally.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show mmrp statistics</td>
<td>Displays the MMRP statistics for an interface or globally.</td>
<td>PE or GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

MVRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode\textsuperscript{a}</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mmrp statistics</td>
<td>Clears the MVRP statistics for an interface or all interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>mmrp</td>
<td>Enables MVRP on a specific interface.</td>
<td>IC or IR</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode⁸</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>mmrp global</td>
<td>Globally enables MVRP.</td>
<td>GC</td>
</tr>
<tr>
<td>mmrp periodic state machine</td>
<td>Globally enables the MVRP periodic state machine.</td>
<td>GC</td>
</tr>
<tr>
<td>show mmrp</td>
<td>Displays the MVRP configuration for an interface or globally.</td>
<td>PE</td>
</tr>
<tr>
<td>show mmrp statistics</td>
<td>Displays the MVRP statistics for an interface or globally.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**MSRP**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear msrp statistics</td>
<td>Clears the MSRP statistics for an interface or all interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>msrp (Interface)</td>
<td>Enables MSRP on a specific interface.</td>
<td>IC</td>
</tr>
<tr>
<td>msrp boundary-propagate</td>
<td>Configures the IEEE 802.1Qav boundary propagation.</td>
<td>GC</td>
</tr>
<tr>
<td>msrp delta-bw</td>
<td>Configures the MSRP VLAN ID for the SR traffic class on the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>msrp global</td>
<td>Globally enables MSRP.</td>
<td>GC</td>
</tr>
<tr>
<td>msrp max-fan-in-ports</td>
<td>Configures the fan-in value used in calculating available bandwidth.</td>
<td>GC</td>
</tr>
<tr>
<td>msrp srclass-pvid</td>
<td>Configures the MSRP VLAN ID for the SR traffic class on the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>msrp srclassqav</td>
<td>Configures the IEEE 802.1Qav class priority map.</td>
<td>GC</td>
</tr>
<tr>
<td>msrp talker-pruning</td>
<td>Enables source pruning.</td>
<td>GC</td>
</tr>
<tr>
<td>show msrp</td>
<td>Displays the MSRP configuration for an interface or globally.</td>
<td>PE</td>
</tr>
<tr>
<td>show msrp reservations</td>
<td>Displays the MSRP reservation information for an interface.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### 802.1AS Timesync

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dot1as statistics</td>
<td>Clears the IEEE 802.1AS statistics for an interface or all interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>dot1x dynamic-vlan enable</td>
<td>Globally enables IEEE 802.1AS.</td>
<td>GC</td>
</tr>
<tr>
<td>dot1as (Interface Configuration)</td>
<td>Enables IEEE 802.1AS on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as priority</td>
<td>Globally configures the priority 1 or priority 2 value.</td>
<td>GC</td>
</tr>
<tr>
<td>dot1as interval announce</td>
<td>Configures the initial log announcement interval for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as interval sync</td>
<td>Configures the sync interval for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as interval pdelay</td>
<td>Configures the pdelay interval for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as timeout announce</td>
<td>Configures the number of announce intervals expiries with no received announce message in which case the master is considered to be no longer transmitting.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as timeout sync</td>
<td>Configures the number of sync intervals expiries with no received announce message in which case the master is considered to be no longer transmitting.</td>
<td>IC</td>
</tr>
<tr>
<td>dot1as pdelay-threshold</td>
<td>Configures the propagation delay threshold in nanoseconds, above which an interface is not considered capable of participating in the 802.1AS protocol.</td>
<td>IC</td>
</tr>
</tbody>
</table>

^a. For the meaning of each Mode abbreviation, see Mode Types.
Data Center Commands

Data Center Bridging

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1as interval pdelay-loss</td>
<td>Configures the number of Pdelay_REQ messages for which a valid response has not been received, above which a port is considered to not be exchanging peer delay messages with its neighbor.</td>
<td>IC</td>
</tr>
<tr>
<td>show dot1as</td>
<td>Displays the IEEE 802.1AS configuration for an interface or globally.</td>
<td>PE</td>
</tr>
<tr>
<td>show dot1as statistics</td>
<td>Displays the IEEE 802.1AS statistics for an interface.</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a For the meaning of each Mode abbreviation, see Mode Types.

For the meaning of each Mode abbreviation, see Mode Types.
### Dell EMC Networking CLI

#### OpenFlow

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-class-group min-bandwidth</td>
<td>Specifies the minimum transmission bandwidth guaranteed for each TCG before processing frames from other TCGs on an interface.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>traffic-class-group strict</td>
<td>Activates the strict priority scheduler mode for each specified TCG.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>traffic-class-group weight</td>
<td>Specifies the scheduling weight for each TCG.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>show classofservice traffic-class-group</td>
<td>Displays the Traffic Class to Traffic Class Group mapping.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces traffic</td>
<td>Displays traffic information.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces traffic-class-group</td>
<td>Displays the Traffic Class to Traffic Class Group mapping.</td>
<td>PE</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

---

## OpenFlow

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller</td>
<td>Configures a connection to an OpenFlow controller</td>
<td>OFC</td>
</tr>
<tr>
<td>hardware profile openflow</td>
<td>Selects the forwarding mode for the OpenFlow hybrid capability.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv4 address</td>
<td>Assigns the IPv4 source address utilized for controller connections.</td>
<td>OFC</td>
</tr>
<tr>
<td>mode</td>
<td>Configures the selection of interfaces used to assign the IP address utilized for controller connections.</td>
<td>OFC</td>
</tr>
<tr>
<td>openflow</td>
<td>Enables OpenFlow on the switch (if disabled) and enters into OpenFlow configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>passive</td>
<td>Sets the switch to wait for the controller to initiate the connection.</td>
<td>OFC</td>
</tr>
<tr>
<td>protocol-version</td>
<td>Selects the version of the protocol in which to operate.</td>
<td>OFC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.
Priority Flow Control

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Bridging Capability Exchange Commands</td>
<td>Enables Priority-Flow-Control (PFC) on an interface.</td>
<td>DCB</td>
</tr>
<tr>
<td>priority-flow-control priority</td>
<td>Enables the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface.</td>
<td>DCB</td>
</tr>
<tr>
<td>clear priority-flow-control statistics</td>
<td>Clears all or interface Priority-Flow-Control statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces priority-flow-control</td>
<td>Displays the global or interface priority flow control status and statistics.</td>
<td>PE</td>
</tr>
</tbody>
</table>

Layer 3 Routing Commands

ARP (IPv4)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Creates an Address Resolution Protocol (ARP) entry.</td>
<td>GC</td>
</tr>
<tr>
<td>arp cachesize</td>
<td>Configures the maximum number of entries in the ARP cache.</td>
<td>GC</td>
</tr>
<tr>
<td>arp dynamicrenew</td>
<td>Enables the ARP component to automatically renew dynamic ARP entries when they age out.</td>
<td>GC</td>
</tr>
<tr>
<td>arp purge</td>
<td>Causes the specified IP address to be removed from the ARP cache.</td>
<td>PE</td>
</tr>
<tr>
<td>arp resptime</td>
<td>Configures the ARP request response timeout.</td>
<td>GC</td>
</tr>
</tbody>
</table>
### Command Description Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp retries</td>
<td>Configures the ARP count of maximum request for retries.</td>
<td>GC</td>
</tr>
<tr>
<td>arp timeout</td>
<td>Configures the ARP entry age-out time.</td>
<td>GC</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>Removes all ARP entries of type dynamic from the ARP cache.</td>
<td>PE</td>
</tr>
<tr>
<td>clear arp-cache management</td>
<td>Removes all entries from the ARP cache learned from the management port.</td>
<td>PE</td>
</tr>
<tr>
<td>ip local-proxy-arp</td>
<td>Enables proxying of ARP requests.</td>
<td>IC</td>
</tr>
<tr>
<td>ip proxy-arp</td>
<td>Enables proxy ARP on a router interface.</td>
<td>IC</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays the Address Resolution Protocol (ARP) cache.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**BFD**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature bfd</td>
<td>Enables BFD on the router.</td>
<td>GC</td>
</tr>
<tr>
<td>bfd echo</td>
<td>Enables BFD echo mode on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>bfd interval</td>
<td>Configures BFD session parameters for a VLAN routing interface.</td>
<td>IC</td>
</tr>
<tr>
<td>bfd slow-timer</td>
<td>Configures the BFD periodic slow transmission interval for BFD Control packets.</td>
<td>GC</td>
</tr>
<tr>
<td>ip ospf bfd</td>
<td>Enable sending of BFD events to OSPF on a VLAN routing interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf bfd</td>
<td>Enables sending of BFD events to OSPF on a VLAN routing interface.</td>
<td>IC</td>
</tr>
<tr>
<td>neighbor fall-over bfd</td>
<td>Enables BFD support for a BGP neighbor.</td>
<td>RBC</td>
</tr>
<tr>
<td>show bfd neighbor</td>
<td>Displays the neighbors for which BFD has established adjacencies.</td>
<td>PE or GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
## BGP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp</td>
<td>Enables BGP and identify the autonomous system (AS) number for the router.</td>
<td>GC</td>
</tr>
<tr>
<td>address-family</td>
<td>Configures policy parameters within a peer template to be applied to a specific address family</td>
<td>PTC</td>
</tr>
<tr>
<td>address-family ipv4 vrf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address-family ipv6</td>
<td>Specifies IPv6 configuration parameters.</td>
<td>BR</td>
</tr>
<tr>
<td>aggregate-address</td>
<td>Configures a summary address for BGP.</td>
<td>BR or IPAF</td>
</tr>
<tr>
<td>bgp aggregate-different-meds (BGP Router Configuration)</td>
<td>Controls the aggregation of routes with different multi-exit discriminator (MED) attributes.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp aggregate-different-meds (IPv6 Address Family Configuration)</td>
<td>Allows IPv6 routes with different MEDs to be aggregated.</td>
<td>IPAF</td>
</tr>
<tr>
<td>bgp always-compare-med</td>
<td>Compares MED values during the decision process in paths received from different autonomous systems.</td>
<td>BR, IPAF</td>
</tr>
<tr>
<td>bgp client-to-client reflection (BGP Router Configuration)</td>
<td>Enables client-to-client reflection.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp client-to-client reflection (IPv6 Address Family Configuration)</td>
<td>Enables client-to-client reflection.</td>
<td>IPAF</td>
</tr>
<tr>
<td>bgp cluster-id</td>
<td>Specifies the cluster ID of a route reflector.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp default local-preference</td>
<td>Enables the network operator to specify the default local preference.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp fast-external-fallover</td>
<td>Configures BGP to immediately reset the adjacency with an external peer if the routing interface to the peer goes down.</td>
<td>BR</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>bgp fast-internal-fallover</td>
<td>Configures BGP to immediately reset the adjacency with an internal peer when there is a loss of reachability to an internal peer.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp listen</td>
<td>Creates an IPv4 listen range and associates it with the specified peer template.</td>
<td>BR, IPAF</td>
</tr>
<tr>
<td>bgp log-neighbor-changes</td>
<td>Enables logging of adjacency state changes.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp maxas-limit</td>
<td>Specifies a limit on the length of AS Paths that BGP accepts from its neighbors.</td>
<td>BR</td>
</tr>
<tr>
<td>bgp router-id</td>
<td>Sets the BGP router ID.</td>
<td>BR</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>Resets peering sessions with all of a subnet of BGP peers.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip bgp counters</td>
<td>Resets all BGP counters to 0.</td>
<td>PE</td>
</tr>
<tr>
<td>default-information originate (BGP Router Configuration)</td>
<td>Enables BGP to originate a default route.</td>
<td>BR</td>
</tr>
<tr>
<td>default-information originate (IPv6 Address Family Configuration)</td>
<td>Allows BGP to originate an IPv6 default route.</td>
<td>IPAF</td>
</tr>
<tr>
<td>default metric (BGP Router Configuration)</td>
<td>Sets the value of the MED attribute on routes redistributed into BGP when no metric has been specified.</td>
<td>BR</td>
</tr>
<tr>
<td>default metric (IPv6 Address Family Configuration)</td>
<td>Sets the metric of redistributed IPv6 routes when a metric is not configured in the redistribute command.</td>
<td>IPAF</td>
</tr>
<tr>
<td>distance</td>
<td>Sets the preference of BGP routes to specific destinations.</td>
<td>IPAF</td>
</tr>
<tr>
<td>distance bgp (BGP Router Configuration)</td>
<td>Sets the preference of BGP routes.</td>
<td>BR</td>
</tr>
<tr>
<td>distance bgp (IPv6 Address Family Configuration)</td>
<td>Sets the preference of BGP routes.</td>
<td>IPAF</td>
</tr>
<tr>
<td>distribute-list prefix in</td>
<td>Configures a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.</td>
<td>BR, IPAF</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>distribute-list prefix out (BGP Router</td>
<td>Configures a filter that restricts the advertisement of routes based on</td>
<td>BR</td>
</tr>
<tr>
<td>Configuration)</td>
<td>destination prefix.</td>
<td></td>
</tr>
<tr>
<td>distribute-list prefix out (IPv6 Address</td>
<td>Applies an IPv6 prefix list to IPv6 routes advertised via BGP.</td>
<td>IPAF</td>
</tr>
<tr>
<td>Family Configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Globally enables BGP.</td>
<td>BR</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>Creates an AS path access list.</td>
<td>GC</td>
</tr>
<tr>
<td>ip bgp-community new-format</td>
<td>Displays BGP standard communities in AA:NN format.</td>
<td>GC</td>
</tr>
<tr>
<td>ip bgp fast-external-failover</td>
<td>Configures fast external failover behavior for a specific routing interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip community-list</td>
<td>Creates or configures a BGP community list.</td>
<td>GC</td>
</tr>
<tr>
<td>ip extcommunity-list</td>
<td>Creates an extended community list to configure VRF route filtering.</td>
<td>GC</td>
</tr>
<tr>
<td>match extcommunity</td>
<td>Matches BGP extended community list attributes.</td>
<td>RM</td>
</tr>
<tr>
<td>maximum-paths (BGP Router Configuration)</td>
<td>Specifies the maximum number of next hops BGP may include in an Equal Cost</td>
<td>BR</td>
</tr>
<tr>
<td></td>
<td>Multipath (ECMP) route derived from paths received from neighbors outside</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the local autonomous system.</td>
<td></td>
</tr>
<tr>
<td>maximum-paths (IPv6 Address Family</td>
<td>Limits the number of ECMP next hops in IPv6 routes from external peers.</td>
<td>IPAF</td>
</tr>
<tr>
<td>Configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>maximum-paths ibgp (BGP Router Configuration)</td>
<td>Specifies the maximum number of next hops BGP may include in an Equal Cost</td>
<td>BR</td>
</tr>
<tr>
<td></td>
<td>Multipath (ECMP) route derived from paths received from neighbors within</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the local autonomous system.</td>
<td></td>
</tr>
<tr>
<td>maximum-paths ibgp (IPv6 Address Family</td>
<td>Limits the number of ECMP next hops in IPv6 routes from internal peers.</td>
<td>IPAF</td>
</tr>
<tr>
<td>Configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode(^a)</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>neighbor activate</td>
<td>Enables the exchange of IPv6 routes with a neighbor.</td>
<td>IPAf, IPAf4</td>
</tr>
<tr>
<td>neighbor advertisement-interval (BGP Router Configuration)</td>
<td>Configures the minimum time that must elapse between advertisements of the same route to a given neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor advertisement-interval (IPv6 Address Family Configuration)</td>
<td>Controls the time between sending Update messages containing IPv6 routes.</td>
<td>IPAf</td>
</tr>
<tr>
<td>neighbor allowas-in</td>
<td>Configures BGP to accept prefixes even if the local ASN is part of the AS_PATH.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor connect-retry-interval</td>
<td>Configure the initial connection retry time for a specific neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor default-originate (BGP Router Configuration)</td>
<td>Configures BGP to originate a default route to a specific neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor default-originate (IPv6 Address Family Configuration)</td>
<td>Configures BGP to originate a default IPv6 route to a specific neighbor.</td>
<td>IPAf</td>
</tr>
<tr>
<td>neighbor description</td>
<td>Records a text description of a neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>Configures BGP to form neighborship with external peers that are not directly connected.</td>
<td>BR, IPAf</td>
</tr>
<tr>
<td>neighbor filter-list (BGP Router Configuration)</td>
<td>Filters advertisements to or from a specific neighbor according to the advertisement’s AS Path.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor filter-list (IPv6 Address Family Configuration)</td>
<td>Filters BGP to apply an AS path access list to UPDATE messages received from or sent to a specific neighbor.</td>
<td>IPAf</td>
</tr>
<tr>
<td>neighbor inherit peer</td>
<td>Configures a BGP peer to inherit peer configuration parameters from a peer template.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor local-as</td>
<td>Configures BGP to advertise the local-as instead of the router’s own AS in the routes advertised to the neighbor.</td>
<td>BR, IPAf</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>neighbor maximum-prefix (BGP Router Configuration)</td>
<td>Configures the maximum number of IPv4 prefixes that BGP will accept from a specified neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor maximum-prefix (IPv6 Address Family Configuration)</td>
<td>Specifies the maximum number of IPv6 prefixes that BGP will accept from a given neighbor.</td>
<td>IPAF</td>
</tr>
<tr>
<td>neighbor next-hop-self (BGP Router Configuration)</td>
<td>Configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor next-hop-self (IPv6 Address Family Configuration)</td>
<td>Configures BGP to use a local address as the IPv6 next hop when advertising IPv6 routes to a specific peer.</td>
<td>IPAF</td>
</tr>
<tr>
<td>neighbor password</td>
<td>Enables MD5 authentication of TCP segments sent to and received from a neighbor, and to configure an authentication key.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor prefix-list (BGP Router Configuration)</td>
<td>Filters advertisements sent to a specific neighbor based on the destination prefix of each route.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor prefix-list (IPv6 Address Family Configuration)</td>
<td>Specifies an IPv6 prefix list to filter routes received from or advertised to a given peer.</td>
<td>IPAF</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Configures a neighbor and identify the neighbor’s autonomous system.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor remove-private-as</td>
<td>Removes private AS numbers when advertising IPv4 routes to an external peer.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor rfc5549-support</td>
<td>Enables advertisement of IPv4 routes over IPv6 next hops selectively to an external BGP IPv6 peer.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor route-map (BGP Router Configuration)</td>
<td>Applies a route map to incoming or outgoing routes for a specific neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor route-map (IPv6 Address Family Configuration)</td>
<td>Specifies a route map to be applied to inbound or outbound IPv6 routes.</td>
<td>IPAF</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>neighbor route-reflector-client (BGP Router Configuration)</td>
<td>Configures an internal peer as an IPv4 route reflector client.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor route-reflector-client (IPv6 Address Family Configuration)</td>
<td>Configures an internal peer as an IPv4 route reflector client.</td>
<td>IPAF</td>
</tr>
<tr>
<td>neighbor send-community (BGP Router Configuration)</td>
<td>Configures the local router to send the BGP communities attribute in UPDATE messages to a specific neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor send-community (IPv6 Address Family Configuration)</td>
<td>Tells BGP to send the COMMUNITIES attribute with routes advertised to the peer.</td>
<td>IPAF</td>
</tr>
<tr>
<td>neighbor shutdown</td>
<td>Administratively disables communications with a specific BGP neighbor.</td>
<td>BR, IPAF</td>
</tr>
<tr>
<td>neighbor timers</td>
<td>Overrides the global keepalive and hold timer values as well as set the keepalive and hold timers for a specific neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>neighbor update-source</td>
<td>Configures BGP to use a specific IP address as the source address for the TCP connection with a neighbor.</td>
<td>BR</td>
</tr>
<tr>
<td>network (BGP Router Configuration)</td>
<td>Configures BGP to advertise an address prefix.</td>
<td>BR</td>
</tr>
<tr>
<td>network (IPv6 Address Family Configuration)</td>
<td>Identifies network IPv6 prefixes that BGP originates in route advertisements to its neighbors.</td>
<td>IPAF</td>
</tr>
<tr>
<td>redistribute (BGP)</td>
<td>Configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, OSPF, and RIP routes.</td>
<td>BR</td>
</tr>
<tr>
<td>redistribute (BGP IPv6)</td>
<td>Configures BGP to redistribute non-BGP routes from the IPv6 routing table.</td>
<td>IPAF</td>
</tr>
<tr>
<td>route-target</td>
<td>Creates a list of export, import, or both route target (RT) extended communities for the specified VRF instance.</td>
<td>PE</td>
</tr>
<tr>
<td>set extcommunity rt</td>
<td>Sets BGP extended community attributes for the route target.</td>
<td>RMC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>set extcommunity soo</td>
<td>Sets BGP extended community attributes for the site of origin.</td>
<td>RMC</td>
</tr>
<tr>
<td>show bgp ipv6</td>
<td>Displays IPv6 routes in the BGP routing table.</td>
<td>UE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GC.</td>
</tr>
<tr>
<td>show bgp ipv6 aggregate-address</td>
<td>Displays the configured IPv6 aggregate addresses and indicates if each address is currently active.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 community</td>
<td>Displays the IPv6 routes that belong to the specified set of communities.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 community-list</td>
<td>Displays the IPv6 routes that match a specified community list.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 listen range</td>
<td>Displays information about IPv6 BGP listen ranges.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 neighbors</td>
<td>Displays neighbors with IPv4 or IPv6 peer addresses that are enabled for the exchange of IPv6 prefixes.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 neighbors advertised-routes</td>
<td>Displays IPv6 routes advertised to a specific neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 neighbors policy</td>
<td>Displays the inbound and outbound IPv6 policies configured for a specific peer.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 neighbors received-routes</td>
<td>Displays a list of IPv6 routes received from a specific neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 statistics</td>
<td>Displays statistics for the IPv6 decision process.</td>
<td>UE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GC.</td>
</tr>
<tr>
<td>show bgp ipv6 summary</td>
<td>Displays a summary of BGP configuration and status.</td>
<td>UE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GC.</td>
</tr>
<tr>
<td>show bgp ipv6 update-group</td>
<td>Reports the status of IPv6 outbound groups and their members.</td>
<td>PE</td>
</tr>
<tr>
<td>show bgp ipv6 route-reflection</td>
<td>Displays a summary of BGP route reflection.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays BGP routes.</td>
<td>UE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td><code>show ip bgp aggregate-address</code></td>
<td>Lists the aggregate addresses that have been configured and indicates whether each is currently active.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp community</code></td>
<td>Displays a BGP community.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp community-list</code></td>
<td>Lists the routes that are allowed by the specified community list.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp extcommunity-list</code></td>
<td>Displays all the permit and deny attributes of the given extended community list.</td>
<td>PE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td><code>show ip bgp listen range</code></td>
<td>Displays information about IPv4 BGP listen ranges.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp neighbors</code></td>
<td>Shows details about BGP neighbor configuration and status.</td>
<td>UE</td>
</tr>
<tr>
<td><code>show ip bgp neighbors advertised-routes</code></td>
<td>Displays the list of routes advertised to a specific neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp neighbors received-routes</code></td>
<td>Displays the list of routes received from a specific neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp neighbors policy</code></td>
<td>Displays the inbound and outbound IPv4 policies configured for a specific peer.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp route-reflection</code></td>
<td>Displays all global configuration related to IPv4 route reflection, including the cluster ID and whether client-to-client route reflection is enabled, and lists all the neighbors that are configured as route reflector clients.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp statistics</code></td>
<td>Displays recent decision process history.</td>
<td>UE</td>
</tr>
<tr>
<td><code>show ip bgp summary</code></td>
<td>Displays a summary of BGP configuration and status.</td>
<td>UE</td>
</tr>
<tr>
<td><code>show ip bgp template</code></td>
<td>Lists the routes that are allowed by the specified community list.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip bgp traffic</code></td>
<td>Lists the routes that are allowed by the specified community list.</td>
<td>UE</td>
</tr>
<tr>
<td><code>show ip bgp update-group</code></td>
<td>Reports the status of IPv4 outbound update groups and their members.</td>
<td>PE</td>
</tr>
</tbody>
</table>
**BGP Routing Policy**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode(^a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp vpn4</td>
<td>Displays the VPNv4 address information from the BGP table.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>template peer</td>
<td>Creates a BGP peer template and enters peer template configuration mode.</td>
<td>BR</td>
</tr>
<tr>
<td>timers bgp</td>
<td>Configures the default keepalive and hold timers that BGP uses for all neighbors unless specifically overridden by the <strong>neighbor timers</strong> command.</td>
<td>BR</td>
</tr>
</tbody>
</table>

\(^a\) For the meaning of each Mode abbreviation, see **Mode Types**.

---

### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode(^a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip as-path access-list</td>
<td>Create an AS path access list.</td>
<td>GC</td>
</tr>
<tr>
<td>ip bgp-community new-format</td>
<td>Displays BGP standard communities in AA:NN format.</td>
<td>GC</td>
</tr>
<tr>
<td>ip community-list</td>
<td>Creates or configures a BGP community list.</td>
<td>GC</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates a prefix list or adds a prefix list entry.</td>
<td>GC</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Applies a text description to a prefix list.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>Creates an IPv6 prefix list or add an IPv6 prefix list entry.</td>
<td>GC</td>
</tr>
<tr>
<td>match as-path</td>
<td>Adds criteria that matches BGP autonomous system paths against an AS path access list to a route map.</td>
<td>RM</td>
</tr>
<tr>
<td>match community</td>
<td>Configures a route map to match based on a BGP community list.</td>
<td>RM</td>
</tr>
<tr>
<td>match ip address prefix-list</td>
<td>Configures a route map to match based on a destination prefix.</td>
<td>RM</td>
</tr>
<tr>
<td>match ipv6 address prefix-list</td>
<td>Configures a route map to match based on an IPv6 destination prefix.</td>
<td>RM</td>
</tr>
<tr>
<td>show ip as-path-access-list</td>
<td>Displays the contents of AS path access lists.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show ip community-list</td>
<td>Displays the contents of AS path access lists.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays the contents of IPv4 prefix lists.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Displays the contents of IPv6 prefix lists.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the IPv4 prefix-list counters.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ipv6 prefix-list</td>
<td>Resets the IPv6 prefix-list counters.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip community-list</td>
<td>Resets the IPv6 prefix-list counters.</td>
<td>PE</td>
</tr>
<tr>
<td>set as-path</td>
<td>Prepends one or more AS numbers to the AS path in a BGP route.</td>
<td>RC</td>
</tr>
<tr>
<td>set comm-list delete</td>
<td>Removes BGP communities from an inbound or outbound UPDATE message.</td>
<td>RM</td>
</tr>
<tr>
<td>set community</td>
<td>Modifies the communities attribute of matching routes.</td>
<td>RM</td>
</tr>
<tr>
<td>set ipv6 next-hop (BGP)</td>
<td>Sets the IPv6 next hop of a route.</td>
<td>RM</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Sets the local preference of specific BGP routes.</td>
<td>RM</td>
</tr>
<tr>
<td>set metric</td>
<td>Sets the metric of a route.</td>
<td>RM</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**DHCP Server and Relay Agent (IPv4)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp pool</td>
<td>Defines a DHCP address pool that can be used to supply addressing information to DHCP client. This command puts the user into DHCP Pool Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>bootfile</td>
<td>Sets the name of the image for the DHCP client to load.</td>
<td>DP</td>
</tr>
<tr>
<td>clear ip dhcp binding</td>
<td>Removes automatic DHCP server bindings.</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip dhcp conflict</td>
<td>Removes DHCP server address conflicts.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>client-identifier</td>
<td>Identifies a Microsoft® DHCP client to be manually assigned an address.</td>
<td>DP</td>
</tr>
<tr>
<td>client-name</td>
<td>Specifies the host name of a DHCP client.</td>
<td>DP</td>
</tr>
<tr>
<td>default-router</td>
<td>Sets the IPv4 address of one or more routers for the DHCP client to use.</td>
<td>DP</td>
</tr>
<tr>
<td>dns-server (IP DHCP Pool Config)</td>
<td>Sets the IPv4 DNS server address which is provided to a DHCP client by the DHCP server.</td>
<td>DP</td>
</tr>
<tr>
<td>domain-name (IP DHCP Pool Config)</td>
<td>Sets the DNS domain name which is provided to a DHCP client by the DHCP server.</td>
<td>DP</td>
</tr>
<tr>
<td>hardware-address</td>
<td>Specifies the MAC address of a client to be manually assigned an address.</td>
<td>DP</td>
</tr>
<tr>
<td>host</td>
<td>Specifies a manual binding for a DHCP client host.</td>
<td>DP</td>
</tr>
<tr>
<td>ip dhcp bootp automatic</td>
<td>Enables automatic BOOTP address assignments.</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp conflict logging</td>
<td>Enables DHCP address conflict detection.</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp excluded-address</td>
<td>Excludes one or more DHCP addresses from automatic assignment.</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp ping packets</td>
<td>Configures the number of pings sent to detect if an address is in use prior to assigning an address from the DHCP pool.</td>
<td>GC</td>
</tr>
<tr>
<td>lease</td>
<td>Sets the period for which a dynamically assigned DHCP address is valid.</td>
<td>DP</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures the IPv4 address of the Windows® Internet Naming Service (WINS) for a Microsoft DHCP client.</td>
<td>DP</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Sets the NetBIOS node type for a Microsoft DHCP client.</td>
<td>DP</td>
</tr>
<tr>
<td>network</td>
<td>Defines a pool of IPv4 addresses for distributing to clients.</td>
<td>DP</td>
</tr>
<tr>
<td>next-server</td>
<td>Sets the IPv4 address of the TFTP server to be used during auto-install.</td>
<td>DP</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>option</td>
<td>Supplies arbitrary configuration information to a DHCP client.</td>
<td>DP</td>
</tr>
<tr>
<td>service dhcp</td>
<td>Enables local IPv4 DHCP server on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp</td>
<td>Sets the IPv4 address of the NTP server to be used for time synchronization of the client.</td>
<td>DP</td>
</tr>
<tr>
<td>show ip dhcp binding</td>
<td>Displays the configured DHCP bindings.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp conflict</td>
<td>Displays DHCP address conflicts for all relevant interfaces or a specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp global configuration</td>
<td>Displays the DHCP global configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp pool</td>
<td>Displays the configured DHCP pool or pools.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip dhcp server statistics</td>
<td>Displays the DHCP server binding and message counters.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

a. For the meaning of each Mode abbreviation, see Mode Types.

### DHCPv6

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp</td>
<td>Clears DHCPv6 statistics for all interfaces or for a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>dns-server (IPv6 DHCP Pool Config)</td>
<td>Sets the IPv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server.</td>
<td>v6DP</td>
</tr>
<tr>
<td>domain-name (IPv6 DHCP Pool Config)</td>
<td>Sets the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server.</td>
<td>v6DP</td>
</tr>
<tr>
<td>ipv6 dhcp pool</td>
<td>Enters IPv6 DHCP Pool Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp relay</td>
<td>Configures an interface for DHCPv6 Relay functionality.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 dhcp server</td>
<td>Configures DHCPv6 server functionality on an interface.</td>
<td>IC</td>
</tr>
</tbody>
</table>
### DHCPv6 Snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp snooping binding</td>
<td>Clears all IPv6 DHCP snooping entries.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>clear ipv6 dhcp snooping statistics</td>
<td>Clears all IPv6 DHCP snooping statistics.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>ipv6 dhcp snooping</td>
<td>Globally enables IPv6 DHCP snooping.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping vlan</td>
<td>Enables IPv6 DHCP snooping on a set of VLANs.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping binding</td>
<td>Configures a static IPv6 DHCP snooping binding.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping database</td>
<td>Configures the persistent location of the DHCP snooping database.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping database write-delay</td>
<td>Configures the time period between successive writes of the binding database.</td>
<td>GC</td>
</tr>
</tbody>
</table>

---

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Modea</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp snooping limit</td>
<td>Configures an interface to disable itself if the rate of received DHCP messages exceeds the configured limit.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping log-invalid</td>
<td>Configures the port to log invalid received DHCP messages.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping trust</td>
<td>Configures the port as trusted.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping verify mac-address</td>
<td>Enables the additional verification of the source MAC address with the client hardware address in the received DHCP message.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 verify binding</td>
<td>Configures a static IP source guard binding.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 verify source</td>
<td>Configures an interface to filter incoming traffic from sources that are not present in the DHCP binding database.</td>
<td>IC</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping</td>
<td>Displays the IPv6 DHCP snooping configuration.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping binding</td>
<td>Displays the IPv6 DHCP snooping configuration.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping database</td>
<td>Displays IPv6 DHCP snooping configurations related to database persistency.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping statistics</td>
<td>Displays IPv6 DHCP snooping filtration statistics.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 source binding</td>
<td>Displays the IPv6 source guard configurations on all ports, an individual port, or on a VLAN.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 verify</td>
<td>Displays the IPv6 Source Guard configuration on all interfaces or the specified interface.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 verify source</td>
<td>Displays the IPv6 source guard configurations on all ports.</td>
<td>UE or PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
## DVMRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode(^a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp</td>
<td>Sets the administrative mode of DVMRP in the router to active.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>ip dvmrp metric</td>
<td>Configures the metric for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>show ip dvmrp</td>
<td>Displays the system-wide information for DVMRP.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dvmrp interface</td>
<td>Displays the interface information for DVMRP on the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dvmrp neighbor</td>
<td>Displays the neighbor information for DVMRP.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dvmrp nexthop</td>
<td>Displays the next hop information on outgoing interfaces for routing multicast datagrams.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dvmrp prune</td>
<td>Displays the table that lists the router’s upstream prune information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dvmrp route</td>
<td>Displays the multicast routing information for DVMRP.</td>
<td>PE</td>
</tr>
</tbody>
</table>

\(^a\) For the meaning of each Mode abbreviation, see [Mode Types](#).

## GMRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode(^a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmrp enable</td>
<td>Enables GMRP globally or on a port.</td>
<td>GC or IC</td>
</tr>
<tr>
<td>clear gvrp statistics</td>
<td>Clears all the GMRO statistics information.</td>
<td>PE</td>
</tr>
<tr>
<td>show gmrp configuration</td>
<td>Displays GMRP configuration.</td>
<td>GC or IC</td>
</tr>
</tbody>
</table>

\(^a\) For the meaning of each Mode abbreviation, see [Mode Types](#).
## IGMP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp last-member-query-count</td>
<td>Sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp last-member-query-interval</td>
<td>Configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp mroute-proxy</td>
<td>Configures downstream IGMP proxy on the selected VLAN interface associated with multicast hosts.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp query-interval</td>
<td>Configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp query-max-response-time</td>
<td>Configures the maximum response time interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp robustness</td>
<td>Configures the robustness that allows tuning of the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp startup-query-count</td>
<td>Sets the number of queries sent out on startup—at intervals equal to the startup query interval for the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp startup-query-interval</td>
<td>Sets the interval between general queries sent at startup on the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp version</td>
<td>Configures the version of IGMP for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>show ip igmp</td>
<td>Displays system-wide IGMP information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp groups</td>
<td>Displays the registered multicast groups on the interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp interface</td>
<td>Displays the IGMP information for the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp membership</td>
<td>Displays the list of interfaces that have registered in the multicast group.</td>
<td>PE</td>
</tr>
</tbody>
</table>
**IGMP Proxy**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arp</code></td>
<td>Enables the IGMP Proxy on the router.</td>
<td>IC</td>
</tr>
<tr>
<td><code>ip igmp proxy-service reset-status</code></td>
<td>Resets the host interface status parameters of the IGMP Proxy router.</td>
<td>IC</td>
</tr>
<tr>
<td><code>ip igmp proxy-service unsolicit-rprt-interval</code></td>
<td>Sets the unsolicited report interval for the IGMP Proxy router.</td>
<td>IC</td>
</tr>
<tr>
<td><code>show ip igmp proxy-service</code></td>
<td>Displays a summary of the host interface status parameters.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip igmp proxy-service interface</code></td>
<td>Displays a detailed list of the host interface status parameters.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip igmp-proxy groups</code></td>
<td>Displays a table of information about multicast groups that IGMP Proxy reported.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip igmp proxy-service groups detail</code></td>
<td>Displays complete information about multicast groups that IGMP Proxy has reported.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

**IP Helper/DHCP Relay**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bootpdhcprelay maxhopcount</code></td>
<td>Configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.</td>
<td>GC</td>
</tr>
<tr>
<td><code>bootpdhcprelay minwaittime</code></td>
<td>Configures the minimum wait time in seconds for BootP/DHCP Relay on the system.</td>
<td>GC</td>
</tr>
<tr>
<td><code>clear ip helper statistics</code></td>
<td>Resets (to 0) the statistics displayed in show ip helper statistics.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

*a. For the meaning of each Mode abbreviation, see Mode Types.*
### IP Routing

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>Configures the link layer encapsulation type for the packet.</td>
<td>IC</td>
</tr>
<tr>
<td>ip icmp echo-reply</td>
<td>Configures an IP address on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ip netdirbcast</td>
<td>Enables the forwarding of network-directed broadcasts.</td>
<td>IC</td>
</tr>
<tr>
<td>ip policy route-map</td>
<td>Applies a route map on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip redirects</td>
<td>Enables the generation of ICMP Redirect messages.</td>
<td>IC</td>
</tr>
<tr>
<td>ip route</td>
<td>Configures a static route. Use the no form of the command to delete the static route.</td>
<td>GC</td>
</tr>
<tr>
<td>ip route default</td>
<td>Configures the default route. Use the no form of the command to delete the default route.</td>
<td>GC</td>
</tr>
<tr>
<td>ip route distance</td>
<td>Sets the default distance (preference) for static routes.</td>
<td>GC</td>
</tr>
<tr>
<td>ip routing</td>
<td>Globally enables IPv4 routing on the router.</td>
<td>GC</td>
</tr>
<tr>
<td>ip unnumbered</td>
<td>Identifies an interface as an unnumbered interface and specifies the numbered interface providing the borrowed address.</td>
<td>IC</td>
</tr>
<tr>
<td>ip unnumbered gratuitous-</td>
<td>Enables installation of a static interface route to the unnumbered peer upon receiving a gratuitous ARP.</td>
<td>IC</td>
</tr>
<tr>
<td>ip unreachables</td>
<td>Enables the generation of ICMP Destination Unreachable messages.</td>
<td>IC</td>
</tr>
<tr>
<td>match ip address</td>
<td>Specify IP address match criteria for a route map.</td>
<td>RM</td>
</tr>
<tr>
<td>match length</td>
<td>Configures packet length matching criteria for a route map.</td>
<td>RM</td>
</tr>
<tr>
<td>match mac-list</td>
<td>Configures MAC ACL match criteria for a route map.</td>
<td>RM</td>
</tr>
<tr>
<td>route-map</td>
<td>Creates a policy based route map.</td>
<td>GC</td>
</tr>
<tr>
<td>set interface null0</td>
<td>Routes packets to interface null 0.</td>
<td>RM</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>Sets a list of default next-hop IP addresses to be used if no explicit route for the packet’s destination address appears in the routing table.</td>
<td>RM</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Specifies the adjacent next-hop router in the path toward the destination to which the packets should be forwarded.</td>
<td>RM</td>
</tr>
<tr>
<td>set ip precedence</td>
<td>Sets the IP precedence bits in the IP packet header.</td>
<td>RM</td>
</tr>
<tr>
<td>show ip brief</td>
<td>Displays all the summary information of the IP.</td>
<td>PE</td>
</tr>
<tr>
<td>Maximum Next Hops.................. 16</td>
<td>Displays all pertinent information about the IP interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip policy</td>
<td>Displays the route maps used for policy based routing on the router interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays the parameters and current state of the active routing protocols.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the routing table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route static</td>
<td>Displays the configured routes, whether or not they are reachable.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route preferences</td>
<td>Displays detailed information about the route preferences.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Shows the number of all routes, including best and non-best routes.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip traffic</td>
<td>Displays IP statistical information.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip vlan</td>
<td>Displays the VLAN routing information for all VLANs with routing enabled.</td>
<td>PE</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays the route maps.</td>
<td>PE</td>
</tr>
<tr>
<td>show routing heap summary</td>
<td>Displays a summary of the memory allocation from the routing heap.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

### IPv6 Routing

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Clears all entries in the IPv6 neighbor table or an entry on a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>clear ipv6 statistics</td>
<td>Clears IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>Configures an IPv6 address on an interface (including tunnel and loopback interfaces).</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>Enables IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 hop-limit</td>
<td>Configures the hop limit used in IPv6 PDUs originated by the router.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 host</td>
<td>Defines static host name-to-IPv6 address mapping in the host cache.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld last-member-</td>
<td>Sets the number of listener-specific queries sent before the router assumes that there are no local members on the interface.</td>
<td>IC (VC)</td>
</tr>
</tbody>
</table>
query-count                  |                                                                                                |       |
| ipv6 mld last-member-       | Sets the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group specific queries sent out of this interface. | IC (VC) |
query-interval               |                                                                                                |       |
| ipv6 mld host-proxy         | Enables MLD Proxy on the router.                                                               | IC    |
| ipv6 mld host-proxy reset-  | Resets the host interface status parameters of the MLD Proxy router.                           | IC    |
status                       |                                                                                                |       |
| ipv6 mld host-proxy unsolicit-rprt-interval | Sets the unsolicited report interval for the MLD Proxy router.                              | IC    |
| ipv6 mld query-interval     | Sets the MLD router’s query interval for the interface.                                        | IC    |
| ipv6 mld query-max-         | Sets MLD querier's maximum response time for the interface.                                   | IC    |
response-time                |                                                                                                |       |
<p>| ipv6 nd dad attempts        | Sets the number of duplicate address detection probes transmitted while doing neighbor discovery. | IC    |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd managed-config-flag</td>
<td>Sets the managed address configuration flag in router advertisements.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd ns-interval</td>
<td>Sets the interval between router advertisements for advertised neighbor solicitations.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd nud max-multicast-solicits</td>
<td>Configures the maximum number of multicast neighbor solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection).</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd nud max-unicast-solicits</td>
<td>Configures the maximum number of unicast neighbor solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection).</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd nud retry</td>
<td>Configures the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachability detection) following the exponential backoff algorithm.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd other-config-flag</td>
<td>Sets the other stateful configuration flag in router advertisements sent from the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd prefix</td>
<td>Sets the IPv6 prefixes to include in the router advertisement.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd raguard attach-policy</td>
<td>Enables RA Guard policy on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd ra-interval</td>
<td>Sets the transmission interval between router advertisements.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd ra-lifetime</td>
<td>Sets the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd reachable-time</td>
<td>Sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode^a</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>ipv6 nd suppress-ra</td>
<td>Suppresses router advertisement transmission on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 redirect</td>
<td>Enables sending IPv6 ICMP redirect messages to peers/hosts when a better first-hop node exists on the path to a destination.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 route</td>
<td>Configures an IPv6 static route</td>
<td>GC</td>
</tr>
<tr>
<td>ip route distance</td>
<td>Sets the default distance (preference) for static routes.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enables forwarding of IPv6 unicast datagrams.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 unreachables</td>
<td>Enables the generation of ICMPv6 Destination Unreachable messages.</td>
<td>IC</td>
</tr>
<tr>
<td>show ipv6 brief</td>
<td>Displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Shows the usability status of IPv6 interfaces.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>Displays information about multicast groups that MLD reported.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>Displays MLD related information for an interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld host-proxy</td>
<td>Displays a summary of the host interface status parameters.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld host-proxy groups</td>
<td>Displays information about multicast groups that the MLD Proxy reported.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld host-proxy groups detail</td>
<td>Displays information about multicast groups that MLD Proxy reported.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld host-proxy interface</td>
<td>Displays a detailed list of the host interface status parameters.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld traffic</td>
<td>Displays MLD statistical information for the router.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 nd raguard policy</td>
<td>Displays the RA Guard policy on all interfaces for which it is enabled.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Displays information about IPv6 neighbors.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### Command Description Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 protocols</td>
<td>Displays information about the configured IPv6 routing protocols.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays the IPv6 routing table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 route preferences</td>
<td>Shows the preference value associated with the type of route.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 route summary</td>
<td>Displays a summary of the routing table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 snooping counters</td>
<td>Displays the RA guard dropped packet counters.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>Shows traffic and statistics for IPv6 and ICMPv6.</td>
<td>UE</td>
</tr>
<tr>
<td>show ipv6 vlan</td>
<td>Displays IPv6 VLAN routing interface addresses.</td>
<td>PE</td>
</tr>
<tr>
<td>traceroute ipv6</td>
<td>Discovers the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see **Mode Types**.

### Loopback Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Enters the Interface Loopback configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>show interfaces loopback</td>
<td>Displays information about configured loopback interfaces.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see **Mode Types**.

### Multicast

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Adds an administrative scope multicast boundary.</td>
<td>IC</td>
</tr>
<tr>
<td>ip mroute</td>
<td>Creates a static multicast route for a source range.</td>
<td>GC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ip multicast-routing</td>
<td>Sets the administrative mode of the IP multicast forwarder in the router to active.</td>
<td>GC</td>
</tr>
<tr>
<td>ip multicast ttl-threshold</td>
<td>Applies a ttlvalue to a routing interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim</td>
<td>Administratively configures PIM mode for IP multicast routing on a VLAN interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim bsr-border</td>
<td>Administratively disables bootstrap router (BSR) messages from being sent or received through an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim bsr-candidate</td>
<td>Configures the router to advertise itself as a bootstrap router (BSR).</td>
<td>GC</td>
</tr>
<tr>
<td>ip pim dense-mode</td>
<td>Administratively configures PIM dense mode for IP multicast routing.</td>
<td>GC</td>
</tr>
<tr>
<td>ip pim dr-priority</td>
<td>Administratively configures the advertised designated router (DR) priority value.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim hello-interval</td>
<td>Administratively configures the PIM Hello messages on the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim join-prune-interval</td>
<td>Administratively configures the frequency of join/prune messages on the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim rp-address</td>
<td>Defines the address of a PIM RP for a specific multicast group range.</td>
<td>GC</td>
</tr>
<tr>
<td>ip pim rp-candidate</td>
<td>Configures the router to advertise itself to the bootstrap router (BSR) as a PIM candidate rendezvous point (RP) for a specific multicast group range.</td>
<td>IC</td>
</tr>
<tr>
<td>ip pim sparse-mode</td>
<td>Administratively configures PIM sparse mode for IP multicast routing.</td>
<td>GC</td>
</tr>
<tr>
<td>ip pim ssm</td>
<td>Administratively configures PIM Source Specific Multicast (SSM) range of addresses for IP multicast routing.</td>
<td>GC</td>
</tr>
<tr>
<td>show ip multicast</td>
<td>Displays the system-wide multicast information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip pim boundary</td>
<td>Displays the system-wide multicast information.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Modea</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>show ip multicast interface</td>
<td>Displays the multicast information for the specified interface.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip mroute</td>
<td>Displays a summary or all the details of the multicast table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip mroute group</td>
<td>Displays the multicast configuration settings of entries in the multicast mroute table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip mroute source</td>
<td>Displays the multicast configuration settings of entries in the multicast mroute table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip mroute static</td>
<td>Displays all the static routes configured in the static mcast table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip pim</td>
<td>Displays information about the interfaces enabled for PIM.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip pim bsr-router</td>
<td>Displays the bootstrap router (BSR) information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip pim interface</td>
<td>Displays PIM interface status parameters. If no interface is specified, the command displays the status parameters of all PIM-enabled interfaces.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip pim neighbor</td>
<td>Displays PIM neighbors discovered by PIMv2 Hello messages. If no interface is specified, the command displays the neighbors discovered on all PIM-enabled interfaces.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip pim rp-hash</td>
<td>Displays the rendezvous point (RP) selected for the specified group address.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip pim rp mapping</td>
<td>Displays the mappings for the PIM group to the active rendezvous points (RPs).</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ip pim statistics</td>
<td>Displays the count of PIM sparse mode received control packets per VLAN.</td>
<td>PE or GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

IPv6 Multicast

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Modea</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 mroute</td>
<td>Selectively clears dynamic IPv6 multicast entries from the cache.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>ipv6 pim (VLAN Interface config)</td>
<td>Administratively enables PIM-SM multicast routing mode on a particular IPv6 router interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 pim bsr-border</td>
<td>Prevents bootstrap router (BSR) messages from being sent or received through an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 pim bsr-candidate</td>
<td>Configures the router to announce its candidacy as a bootstrap router (BSR).</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim dense-mode</td>
<td>Administratively configures PIM dense mode for IPv6 multicast routing.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim dr-priority</td>
<td>Sets the priority value for which a router is elected as the designated router (DR).</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 pim hello-interval</td>
<td>Administratively configures the PIM-SM Hello Interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 pim join-prune-interval</td>
<td>Administratively configures the interface join/prune interval for the PIM-SM router.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 pim register-threshold</td>
<td>Configures the Register Threshold rate for the RP router to switch to the shortest path.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim rp-address</td>
<td>Statically configures the Rendezvous Point (RP) address for one or more multicast groups.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim rp-candidate</td>
<td>Configures the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim sparse-mode</td>
<td>Administratively configures PIM sparse mode for multicast routing.</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 pim ssm</td>
<td>Defines the Source Specific Multicast (SSM) range of multicast addresses.</td>
<td>GC</td>
</tr>
<tr>
<td>show ipv6 pim</td>
<td>Displays global status of IPv6 PIMSM and its IPv6 routing interfaces.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 pim bsr-router</td>
<td>Display the bootstrap router (BSR) information.</td>
<td>UE, PE, or GC</td>
</tr>
<tr>
<td>show ip mroute group</td>
<td>Displays the multicast configuration settings</td>
<td>PE</td>
</tr>
<tr>
<td>show ip mroute source</td>
<td>Displays the multicast configuration settings</td>
<td>PE</td>
</tr>
</tbody>
</table>
**OSPF**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode⁹</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 pim interface</td>
<td>Displays interface config parameters.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 pim neighbor</td>
<td>Displays IPv6 PIMSM neighbors learned on the routing interfaces.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 pim rp-hash</td>
<td>Displays which rendezvous point (RP) is being selected for a specified group.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show ipv6 pim rp mapping</td>
<td>Displays all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)).</td>
<td>PE or GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see **Mode Types**.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>area stub no-summary</td>
<td>Prevents Summary LSAs from being advertised into the NSSA.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link</td>
<td>Creates the OSPF virtual interface for the specified area-id and neighbor router.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link authentication</td>
<td>Configures the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link dead-interval</td>
<td>Configures the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link hello-interval</td>
<td>Configures the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link retransmit-interval</td>
<td>Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>area virtual-link transmit-delay</td>
<td>Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>auto-cost</td>
<td>Allows user to change the reference bandwidth used in computing link cost.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Allows user to change the bandwidth used in computing link cost.</td>
<td>IC</td>
</tr>
<tr>
<td>bfd</td>
<td>Enables processing of BFD events by OSPF on all interfaces enabled for BFD.</td>
<td>RO SPF, RO SV3</td>
</tr>
<tr>
<td>capability opaque</td>
<td>Enables Opaque Capability on the router.</td>
<td>RC</td>
</tr>
<tr>
<td>clear ip ospf</td>
<td>Resets specific OSPF states.</td>
<td>PE</td>
</tr>
<tr>
<td>compatible rfc1583</td>
<td>Enables OSPF 1583 compatibility.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>default-information originate (Router OSPF Configuration)</td>
<td>Controls the advertisement of default routes.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>default-metric</td>
<td>Sets a default for the metric of distributed routes.</td>
<td>RO SPF</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode^a</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>distance ospf</td>
<td>Sets the route preference value of OSPF in the router.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Specifies the access list to filter routes received from the source protocol.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>enable</td>
<td>Resets the default administrative mode of OSPF in the router (active).</td>
<td>ROSPF</td>
</tr>
<tr>
<td>exit-overflow-interval</td>
<td>Configures the exit overflow interval for OSPF.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>external-lsdb-limit</td>
<td>Configures the external LSDB limit for OSPF.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>ip ospf area</td>
<td>Enables OSPFv2 and sets the area ID of an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf authentication</td>
<td>Sets the OSPF Authentication Type and Key for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf cost</td>
<td>Configures the cost on an OSPF interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf database-filter all out</td>
<td>Prevents the flooding of OSPF LSAs on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf dead-intervall</td>
<td>Sets the OSPF dead interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf hello-interval</td>
<td>Sets the OSPF hello interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf mtu-ignore</td>
<td>Disables OSPF maximum transmission unit (MTU) mismatch detection.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf network</td>
<td>Configure OSPF to treat an interface as a point-to-point, rather than broadcast interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf priority</td>
<td>Sets the OSPF priority for the specified router interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf retransmit-interval</td>
<td>Sets the OSPF retransmit Interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip ospf transmit-delay</td>
<td>Sets the OSPF Transit Delay for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>log adjacency-changes</td>
<td>Enables logging of OSPFv2 neighbor state changes.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>max-metric router-lsa</td>
<td>Configures OSPF to enable stub router mode.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>maximum-paths</td>
<td>Sets the number of paths that OSPF can report for a given destination.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>network area</td>
<td>Enables OSPFv2 on an interface and sets its area ID if the IP address of an interface is covered by this network command.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>nsf</td>
<td>Enables OSPF graceful restart.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>nsf helper</td>
<td>Allow OSPF to act as a helpful neighbor for a restarting router.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>nsf helper strict-lsa-checking</td>
<td>Set an OSPF helpful neighbor exit helper mode whenever a topology change occurs.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>nsf restart-interval</td>
<td>Configures the length of the grace period on the restarting router.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>passive-interface</td>
<td>Sets the interface or tunnel as passive.</td>
<td>IC</td>
</tr>
<tr>
<td>passive-interface default</td>
<td>Enables the global passive mode by default for all interfaces.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>passive-interface</td>
<td>Sets the interface or tunnel as passive.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>redistribute (BGP)</td>
<td>Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>router-id</td>
<td>Sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.</td>
<td>ROSPF</td>
</tr>
<tr>
<td>router ospf</td>
<td>Enters Router OSPF mode.</td>
<td>GC</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Displays information relevant to the OSPF router.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip ospf abr</td>
<td>Displays the internal OSPF routing table entries to Area Border Routers (ABR).</td>
<td>PE</td>
</tr>
<tr>
<td>show ip ospf area</td>
<td>Displays information about the identified OSPF area.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip ospf asbr</td>
<td>Displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR).</td>
<td>PE</td>
</tr>
<tr>
<td>show ip ospf database</td>
<td>Displays information about the link state database when OSPF is enabled.</td>
<td>PE</td>
</tr>
</tbody>
</table>
### Command Description Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ospf database database-summary</code></td>
<td>Displays the number of each type of LSA in the database for each area and for the router.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf interface</code></td>
<td>Displays the information for the IFO object or virtual interface tables.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf interface brief</code></td>
<td>Displays brief information for the IFO object or virtual interface tables.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf interface stats</code></td>
<td>Displays the statistics for a specific interface.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf lsa-group</code></td>
<td>Displays the number of self-originated LSAs within each LSA group.</td>
<td>PE, GC</td>
</tr>
<tr>
<td><code>show ip ospf neighbor</code></td>
<td>Displays information about OSPF neighbors.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf range</code></td>
<td>Displays information about the area ranges for the specified area-id.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf statistics</code></td>
<td>Displays information about recent Shortest Path First (SPF) calculations.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf stub table</code></td>
<td>Displays the OSPF stub table.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf virtual-links</code></td>
<td>Displays the OSPF Virtual Interface information for a specific area and neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip ospf virtual-links brief</code></td>
<td>Displays the OSPF Virtual Interface information for all areas in the system.</td>
<td>PE</td>
</tr>
<tr>
<td><code>timers pacing flood</code></td>
<td>Adjusts the rate at which OSPFv2 sends LS Update packets</td>
<td>OG</td>
</tr>
<tr>
<td><code>timers pacing lsa-group</code></td>
<td>Tunes how OSPF groups LSAs for periodic refresh.</td>
<td>OG</td>
</tr>
<tr>
<td><code>timers spf</code></td>
<td>Configures the SPF delay and hold time.</td>
<td>RO SPF</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**OSPFv3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area default-cost (Router OSPFv3)</code></td>
<td>Configures the monetary default cost for the stub area.</td>
<td>RO SPF</td>
</tr>
</tbody>
</table>

Dell EMC Networking CLI | 192
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>area nssa (Router OSPFv3)</td>
<td>Configures the specified areaid to function as an NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area nssa default-info-originate (Router OSPFv3 Config)</td>
<td>Configures the metric value and type for the default route advertised into the NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area nssa no-redistribute</td>
<td>Configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area nssa no-summary</td>
<td>Configures the NSSA so that summary LSAs are not advertised into the NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area nssa translator-role</td>
<td>Configures the translator role of the NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area nssa translator-stab-intv</td>
<td>Configures the translator stability interval of the NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area range (Router OSPFv3)</td>
<td>Creates an area range for a specified NSSA.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area stub</td>
<td>Creates a stub area for the specified area ID.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area stub no-summary</td>
<td>Disables the import of Summary LSAs for the stub area identified by areaid.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area virtual-link</td>
<td>Creates the OSPF virtual interface for the specified areaid and neighbor.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area virtual-link dead-interval</td>
<td>Configures the dead interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area virtual-link hello-interval</td>
<td>Configures the hello interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area virtual-link retransmit-interval</td>
<td>Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>area virtual-link transmit-delay</td>
<td>Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>default-information originate (Router OSPFv3 Configuration)</td>
<td>Controls the advertisement of default routes.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>default-metric</td>
<td>Sets a default for the metric of distributed routes.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>distance ospf</td>
<td>Sets the route preference value of OSPF in the router.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>enable</td>
<td>Resets the default administrative mode of OSPF in the router (active).</td>
<td>ROSV3</td>
</tr>
<tr>
<td>exit-overflow-interval</td>
<td>Configures the exit overflow interval for OSPF.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>external-lsdb-limit</td>
<td>Configures the external LSDB limit for OSPF.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>arp</td>
<td>Enables OSPF on a router interface or loopback interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf area</td>
<td>Sets the OSPF area to which the specified router interface belongs.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf cost</td>
<td>Configures the cost on an OSPF interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf dead-interval</td>
<td>Sets the OSPF dead interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf hello-interval</td>
<td>Sets the OSPF hello interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf mtu-ignore</td>
<td>Disables OSPF maximum transmission unit (MTU) mismatch detection.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf network</td>
<td>Changes the default OSPF network type for the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf priority</td>
<td>Sets the OSPF priority for the specified router interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf retransmit-interval</td>
<td>Sets the OSPF retransmit interval for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 ospf transmit-delay</td>
<td>Sets the OSPF Transmit Delay for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 router ospf</td>
<td>Enters Router OSPFv3 Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>maximum-paths</td>
<td>Sets the number of paths that OSPF can report for a given destination.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>nsf</td>
<td>Enables OSPF graceful restart.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>nsf helper</td>
<td>Allows OSPF to act as a helpful neighbor for a restarting router.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>nsf helper strict-lsa-checking</td>
<td>Requires that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>nsf restart-interval</td>
<td>Configures the length of the grace period on the restarting router.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>passive-interface</td>
<td>Sets the interface or tunnel as passive.</td>
<td>IC</td>
</tr>
<tr>
<td>passive-interface default</td>
<td>Enables the global passive mode by default for all interfaces.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>redistribute (OSPFv3)</td>
<td>Configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>router-id</td>
<td>Sets a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.</td>
<td>ROSV3</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>Displays information relevant to the OSPF router.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf abr</td>
<td>Displays the internal OSPFv3 routes to reach Area Border Routers (ABR).</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf area</td>
<td>Displays information about the area.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf asbr</td>
<td>Displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR).</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf border-routers</td>
<td>Displays internal OSPFv3 routers to reach Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR).</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show ipv6 ospf database</td>
<td>Displays information about the link state database when OSPFv3 is enabled.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf database database-summary</td>
<td>Displays the number of each type of LSA in the database and the total number of LSAs in the database.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf interface</td>
<td>Displays the information for the IFO object or virtual interface tables.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>show ipv6 ospf interface brief</td>
<td>Displays brief information for the IFO object or virtual interface tables.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf interface stats</td>
<td>Displays the statistics for a specific interface.</td>
<td>UE</td>
</tr>
<tr>
<td>show ipv6 ospf interface vlan</td>
<td>Displays OSPFv3 configuration and status information for a specific VLAN.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf neighbor</td>
<td>Displays information about OSPF neighbors.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf range</td>
<td>Displays information about the area ranges for the specified area identifier.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf stub table</td>
<td>Displays the OSPF stub table.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf virtual-links</td>
<td>Displays the OSPF Virtual Interface information for a specific area and neighbor.</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 ospf virtual-link brief</td>
<td>Displays the OSPFV3 Virtual Interface information for all areas in the system.</td>
<td>PE</td>
</tr>
<tr>
<td>timers throttle spf</td>
<td>Throttles the link-state-packets.</td>
<td>OR</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see [Mode Types](#).

### Router Discovery Protocol

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>Enables Router Discovery on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip irdp holdtime</td>
<td>Configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip irdp maxadvertinterval</td>
<td>Configures the maximum time, in seconds, allowed between sending router advertisements from the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip irdp minadvertinterval</td>
<td>Configures the minimum time, in seconds, allowed between sending router advertisements from the interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip irdp multicast</td>
<td>Sends router advertisements as IP multicast packets.</td>
<td>IC</td>
</tr>
</tbody>
</table>
### Routing Information Protocol

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip irdp preference</td>
<td>Configures the preference of the address as a default router address relative to other router addresses on the same subnet.</td>
<td>IC</td>
</tr>
<tr>
<td>show ip irdp</td>
<td>Displays the router discovery information for all interfaces, or for a specified interface.</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

**Command**

**Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-summary</td>
<td>Enables the RIP auto-summarization mode.</td>
<td>RIP</td>
</tr>
<tr>
<td>default-information originate (Router RIP Configuration)</td>
<td>Controls the advertisement of default routes.</td>
<td>RIP</td>
</tr>
<tr>
<td>default-metric</td>
<td>Sets a default for the metric of distributed routes.</td>
<td>RIP</td>
</tr>
<tr>
<td>distance rip</td>
<td>Sets the route preference value of RIP in the router.</td>
<td>RIP</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Specifies the access list to filter routes received from the source protocol.</td>
<td>RIP</td>
</tr>
<tr>
<td>enable</td>
<td>Resets the default administrative mode of RIP in the router (active).</td>
<td>RIP</td>
</tr>
<tr>
<td>hostroutesaccept</td>
<td>Enables the RIP hostroutesaccept mode.</td>
<td>RIP</td>
</tr>
<tr>
<td>ip rip</td>
<td>Enables RIP on a router interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip rip authentication</td>
<td>Sets the RIP Version 2 Authentication Type and Key for the specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td>ip rip receive version</td>
<td>Configures the interface to allow RIP control packets of the specified version(s) to be received.</td>
<td>IC</td>
</tr>
<tr>
<td>ip rip send version</td>
<td>Configures the interface to allow RIP control packets of the specified version to be sent.</td>
<td>IC</td>
</tr>
</tbody>
</table>

---

*a. For the meaning of each Mode abbreviation, see Mode Types.*
### Tunnel Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel</td>
<td>Enables the interface configuration mode for a tunnel.</td>
<td>GC</td>
</tr>
<tr>
<td>show interfaces tunnel</td>
<td>Displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.</td>
<td>PE</td>
</tr>
<tr>
<td>tunnel destination</td>
<td>Specifies the destination transport address of the tunnel.</td>
<td>IC</td>
</tr>
<tr>
<td>tunnel mode ipv6ip</td>
<td>Specifies the mode of the tunnel.</td>
<td>IC</td>
</tr>
<tr>
<td>tunnel source</td>
<td>Specifies the source transport address of the tunnel, either explicitly or by reference to an interface.</td>
<td>IC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

### Virtual Router

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Assigns descriptive text to the VRF instance.</td>
<td>VR</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.
### Command Description Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip vrf</code></td>
<td>Creates a virtual router with a specified name and enters Virtual Router Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td><code>ip vrf forwarding</code></td>
<td>Associates an interface with a VRF instance.</td>
<td>IC or IR</td>
</tr>
<tr>
<td><code>maximum routes</code></td>
<td>Reserves the number of routes allowed and sets the maximum limit on the number of routes for a virtual router instance in the total routing table space for the router.</td>
<td>VR</td>
</tr>
<tr>
<td><code>show ip vrf</code></td>
<td>Shows the interfaces associated with a VRF instance.</td>
<td>PE</td>
</tr>
</tbody>
</table>

*a. For the meaning of each Mode abbreviation, see Mode Types.*

### Virtual Router Redundancy

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip vrrp</code></td>
<td>Enables the administrative mode of Virtual Router Redundancy Protocol (VRRP) for the router.</td>
<td>GC</td>
</tr>
<tr>
<td><code>vrrp accept-mode</code></td>
<td>Enables the VRRP Master to accept ping packets sent to one of the virtual router’s IP addresses.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp authentication</code></td>
<td>Sets the authentication details value for the virtual router configured on a specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp description</code></td>
<td>Assigns a description to the VRRP group.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp ip</code></td>
<td>Sets the virtual router IP address value for an interface.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp mode</code></td>
<td>Enables the virtual router configured on an interface. Enabling the status field starts a virtual router.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp preempt</code></td>
<td>Sets the preemption mode value for the virtual router configured on a specified interface.</td>
<td>IC</td>
</tr>
<tr>
<td><code>vrrp priority</code></td>
<td>Sets the priority value for the virtual router configured on a specified interface.</td>
<td>IC</td>
</tr>
</tbody>
</table>
Switch Management Commands

Application Deployment

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>application install</td>
<td>Installs or removes a Dell-supplied application.</td>
<td>GC</td>
</tr>
<tr>
<td>application start</td>
<td>Schedules a Dell-supplied application for immediate execution on the stack master.</td>
<td>GC</td>
</tr>
<tr>
<td>application stop</td>
<td>Stops a Dell-supplied application if the application is executing on the stack master.</td>
<td>GC</td>
</tr>
<tr>
<td>show application</td>
<td>Displays installed applications and optionally displays application files.</td>
<td>GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
### Auto-Install

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot auto-copy-sw</td>
<td>Enables or disables Stack Firmware Synchronization.</td>
<td>GC</td>
</tr>
<tr>
<td>boot auto-copy-sw allow-downgrade</td>
<td>Enables downgrading the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.</td>
<td>GC</td>
</tr>
<tr>
<td>boot host auto-reboot</td>
<td>Enables rebooting the device (no administrative intervention) when the auto-image is successfully downloaded.</td>
<td>GC</td>
</tr>
<tr>
<td>boot host auto-save</td>
<td>Enables/disables automatically saving the downloaded configuration on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>boot host dhcp</td>
<td>Enables/disables Auto Config on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>boot host retry-count</td>
<td>Set the number of attempts to download a configuration.</td>
<td>GC</td>
</tr>
<tr>
<td>show auto-copy-sw</td>
<td>Displays Stack Firmware Synchronization configuration status.</td>
<td>PE</td>
</tr>
<tr>
<td>show boot</td>
<td>Displays the current status of the Auto Config process.</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a. For the meaning of each Mode abbreviation, see Mode Types.

### CLI Macro

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro name</td>
<td>Creates a user-defined macro.</td>
<td>GC</td>
</tr>
<tr>
<td>macro global apply</td>
<td>Use to apply a macro.</td>
<td>GC</td>
</tr>
<tr>
<td>macro global trace</td>
<td>Applies and traces a macro.</td>
<td>GC</td>
</tr>
<tr>
<td>macro global description</td>
<td>Appends a line to the global macro description.</td>
<td>GC</td>
</tr>
<tr>
<td>macro apply</td>
<td>Use to apply a macro.</td>
<td>IC</td>
</tr>
<tr>
<td>macro trace</td>
<td>Applies and traces a macro.</td>
<td>IC</td>
</tr>
<tr>
<td>macro description</td>
<td>Appends a line to the macro description.</td>
<td>IC</td>
</tr>
<tr>
<td>show parser macro</td>
<td>Displays information about defined macros.</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a. For the meaning of each Mode abbreviation, see Mode Types.
Clock

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snntp configuration</td>
<td>Displays the SNTP configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>show snntp server</td>
<td>Displays the preconfigured SNTP servers.</td>
<td>PE</td>
</tr>
<tr>
<td>show snntp status</td>
<td>Displays the SNTP status.</td>
<td>PE</td>
</tr>
<tr>
<td>sntp authenticate</td>
<td>Set to require authentication for received NTP traffic from servers.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp authentication-key</td>
<td>Defines an authentication key for SNTP.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp broadcast client enable</td>
<td>Enables SNTP Broadcast clients.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp client poll timer</td>
<td>Defines polling time for the SNTP client.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp server</td>
<td>Configures the SNTP server to use SNTP to request and accept NTP traffic from it.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp source-interface</td>
<td>Selects the interface from which to use the IP address in the source IP address field of transmitted SNTP packets.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp trusted-key</td>
<td>Authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize.</td>
<td>GC</td>
</tr>
<tr>
<td>sntp unicast client enable</td>
<td>Enables clients to use Simple Network Time Protocol (SNTP) predefined Unicast clients.</td>
<td>GC</td>
</tr>
<tr>
<td>clock timezone hours-offset</td>
<td>Sets the offset to Coordinated Universal Time.</td>
<td>GC</td>
</tr>
<tr>
<td>no clock timezone</td>
<td>Resets the time zone settings.</td>
<td>GC</td>
</tr>
<tr>
<td>clock summer-time recurring</td>
<td>Sets the summertime offset to UTC recursively every year.</td>
<td>GC</td>
</tr>
<tr>
<td>clock summer-time date</td>
<td>Sets the summertime offset to UTC.</td>
<td>GC</td>
</tr>
<tr>
<td>no clock summer-time</td>
<td>Resets the summertime configuration.</td>
<td>GC</td>
</tr>
<tr>
<td>show clock</td>
<td>Displays the time and date from the system clock.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
## Command Line Configuration Scripting

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>script apply</td>
<td>Applies commands in the script to the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>script delete</td>
<td>Deletes a specific script.</td>
<td>PE</td>
</tr>
<tr>
<td>script list</td>
<td>Lists all scripts present in the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>script show</td>
<td>Displays the contents of a script file.</td>
<td>PE</td>
</tr>
<tr>
<td>script validate</td>
<td>Validates a script file.</td>
<td>PE</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see [Mode Types](#).

## Configuration and Image Files

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot system</td>
<td>Specifies the system image that the switch loads at startup.</td>
<td>PE</td>
</tr>
<tr>
<td>clear config</td>
<td>Restores switch to default configuration.</td>
<td>PE</td>
</tr>
<tr>
<td>copy</td>
<td>Copies files from a source to a destination.</td>
<td>PE</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file from a flash memory.</td>
<td>PE</td>
</tr>
<tr>
<td>dir</td>
<td>Prints the contents of the flash file system.</td>
<td>PE</td>
</tr>
<tr>
<td>erase</td>
<td>Erases the startup configuration, the backup configuration, or the backup image.</td>
<td>PE</td>
</tr>
<tr>
<td>filedescr</td>
<td>Adds a description to a file.</td>
<td>PE</td>
</tr>
<tr>
<td>rename</td>
<td>Renames the file present in flash.</td>
<td>PE</td>
</tr>
<tr>
<td>show backup-config</td>
<td>Displays contents of a backup configuration file.</td>
<td>PE</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the active system image file that the switch loads at startup.</td>
<td>UE</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file.</td>
<td>PE</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the startup configuration file contents.</td>
<td>PE</td>
</tr>
<tr>
<td>write</td>
<td>Copies the running configuration image to the startup configuration.</td>
<td>PE</td>
</tr>
</tbody>
</table>
Dell EMC Networking CLI

DHCP Client

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>release dhcp</td>
<td>Forces the DHCPv4 client to release a leased address.</td>
<td>PE</td>
</tr>
<tr>
<td>renew dhcp</td>
<td>Forces the DHCP client to immediately renew an IPv4 address lane.</td>
<td>PE</td>
</tr>
<tr>
<td>show dhcp lease</td>
<td>Displays IPv4 addresses leased from a DHCP server.</td>
<td>PE</td>
</tr>
</tbody>
</table>

HiveAgent

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>eula-consent</td>
<td>Accepts or declines the end-user license agreement (EULA) for the hive agent</td>
<td>GC</td>
</tr>
<tr>
<td>hiveagent</td>
<td>Accesses the HiveAgent configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>server</td>
<td>Configures a HiveAgent server (HiveManager NG) and enter HiveAgent server configuration mode.</td>
<td>HAC</td>
</tr>
<tr>
<td>debug</td>
<td>Enables HiveAgent debug capability.</td>
<td>HAC</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a HiveAgent server.</td>
<td>HAC</td>
</tr>
<tr>
<td>proxy-ip-address</td>
<td>Configures a proxy server to be used to contact the HiveManager NG.</td>
<td>HAC</td>
</tr>
<tr>
<td>source-interface vlan-id</td>
<td>Assigns a source interface which HiveAgent obtains the IP address used as the source IP address in packets addressed to the HiveManager NG</td>
<td>HAC</td>
</tr>
<tr>
<td>url</td>
<td>Configures the URL to reach on HiveManager NG.</td>
<td>HAC</td>
</tr>
<tr>
<td>show hiveagent debug</td>
<td>Use to view information on HiveAgent debug configuration.</td>
<td>PE, GC</td>
</tr>
</tbody>
</table>

For the meaning of each Mode abbreviation, see Mode Types.
### Line

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>show hiveagent source-interface</td>
<td>Displays the configured HiveAgent source interface.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>show hiveagent status</td>
<td>Displays information on the HiveAgent configuration.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>show eula-consent hiveagent</td>
<td>Reviews the EULA details.</td>
<td>PE, GC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Applies an accounting method to a line config.</td>
<td>LC</td>
</tr>
<tr>
<td>authorization</td>
<td>Applies a command authorization method to a line config.</td>
<td>LC</td>
</tr>
<tr>
<td>enable authentication</td>
<td>Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.</td>
<td>LC</td>
</tr>
<tr>
<td>exec-banner</td>
<td>Enables exec banner on the console, telnet or SSH connection.</td>
<td>LC</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>Configures the interval that the system waits for user input before Privileged Exec mode timeout.</td>
<td>LC</td>
</tr>
<tr>
<td>history</td>
<td>Enables the command history function.</td>
<td>LC</td>
</tr>
<tr>
<td>history size</td>
<td>Changes the command history buffer size for a particular line.</td>
<td>LC</td>
</tr>
<tr>
<td>line</td>
<td>Identifies a specific line for configuration and enters the line configuration command mode.</td>
<td>GC</td>
</tr>
<tr>
<td>login authentication</td>
<td>Specifies the login authentication method list for a remote telnet or console.</td>
<td>LC</td>
</tr>
<tr>
<td>login-banner</td>
<td>Enables login banner on the console, telnet, or SSH connection.</td>
<td>LC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode^a</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>nsf</td>
<td>Enables display of the message of the day banner on the console, telnet, or SSH connection.</td>
<td>LC</td>
</tr>
<tr>
<td>password (Line Configuration)</td>
<td>Specifies a password on a line.</td>
<td>LC</td>
</tr>
<tr>
<td>show line</td>
<td>Displays line parameters.</td>
<td>UE</td>
</tr>
<tr>
<td>speed</td>
<td>Sets the serial port BAUD rate.</td>
<td>LC</td>
</tr>
<tr>
<td>terminal length</td>
<td>Sets the terminal length.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**PHY Diagnostics**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>show copper-ports tdr</td>
<td>Displays the last TDR (Time Domain Reflectometry) tests on specified ports.</td>
<td>PE</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver</td>
<td>Displays the optical transceiver diagnostics.</td>
<td>PE</td>
</tr>
<tr>
<td>test copper-port tdr</td>
<td>Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**Power Over Ethernet (PoE)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode^a</th>
</tr>
</thead>
<tbody>
<tr>
<td>power inline</td>
<td>Enables/disables the ability of the port to deliver power.</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td>power inline detection</td>
<td>Configures the detection type that tells which types of PD’s will be detected and powered by the switch.</td>
<td>IC</td>
</tr>
<tr>
<td>power inline four-pair forced</td>
<td>Forces 4-pair power feed on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>power inline limit</strong></td>
<td>Configure the type of power limit.</td>
<td>IC</td>
</tr>
<tr>
<td><strong>power inline management</strong></td>
<td>Sets the power management type.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>power inline powered-device</strong></td>
<td>Adds a comment or description of the powered device type.</td>
<td>IC   (Ethernet)</td>
</tr>
<tr>
<td><strong>power inline priority</strong></td>
<td>Configures the port priority level for the delivery of power to an attached device.</td>
<td>IC   (Ethernet)</td>
</tr>
<tr>
<td><strong>power inline reset</strong></td>
<td>Use to reset the port.</td>
<td>IC</td>
</tr>
<tr>
<td><strong>power inline usage-threshold</strong></td>
<td>Configures the system power usage threshold level at which lower priority ports are disconnected.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>clear power inline statistics</strong></td>
<td>Clears the PoE statistics.</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show power inline</strong></td>
<td>Reports current PoE configuration and status.</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show power inline firmware-version</strong></td>
<td>Displays the version of the PoE controller firmware present on the switch file system.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see **Mode Types**.

**RMON**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>rmon alarm</strong></td>
<td>Configures alarm conditions.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>rmon collection history</strong></td>
<td>Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.</td>
<td>IC</td>
</tr>
<tr>
<td><strong>rmon event</strong></td>
<td>Configures an RMON event.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>rmon hcalarm</strong></td>
<td>Configures high capacity alarms.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>show rmon alarm</strong></td>
<td>Displays alarm configurations.</td>
<td>UE</td>
</tr>
<tr>
<td><strong>show rmon alarms</strong></td>
<td>Displays the alarms summary table.</td>
<td>UE and PE</td>
</tr>
<tr>
<td><strong>show rmon collection history</strong></td>
<td>Displays the requested group of statistics.</td>
<td>UE</td>
</tr>
<tr>
<td><strong>show rmon events</strong></td>
<td>Displays the RMON event table.</td>
<td>UE</td>
</tr>
<tr>
<td><strong>show rmon hcalarm</strong></td>
<td>Displays the high capacity alarms.</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show rmon history</strong></td>
<td>Displays RMON Ethernet Statistics history.</td>
<td>UE</td>
</tr>
</tbody>
</table>
Serviceability Tracing

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon log</td>
<td>Displays the RMON logging table.</td>
<td>UE</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>Displays RMON Ethernet Statistics.</td>
<td>UE</td>
</tr>
<tr>
<td>debug aaa accounting</td>
<td>Enables debugging for accounting.</td>
<td>PE</td>
</tr>
<tr>
<td>debug arp</td>
<td>Enables tracing of ARP packets.</td>
<td>PE</td>
</tr>
<tr>
<td>debug authentication interface</td>
<td>Enables Authentication Manager debug traces for the interface.</td>
<td>PE</td>
</tr>
<tr>
<td>debug auto-voip</td>
<td>Enables Auto VOIP debug messages.</td>
<td>PE</td>
</tr>
<tr>
<td>debug bfd</td>
<td>Enables the display of BFD events or packets.</td>
<td>PE</td>
</tr>
<tr>
<td>debug cfm</td>
<td>Enables CFM debugging.</td>
<td>PE</td>
</tr>
<tr>
<td>debug clear</td>
<td>Disables all debug traces.</td>
<td>PE</td>
</tr>
<tr>
<td>debug console</td>
<td>Enables the display of debug trace output on the login session in which it is executed.</td>
<td>PE</td>
</tr>
<tr>
<td>debug crashlog</td>
<td>Displays the crash log contents on the console.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>debug dhcp packet</td>
<td>Displays debug information about DHCPv4 client activities and traces DHCP v4 packets to and from the local DHCPv4 client.</td>
<td>PE</td>
</tr>
<tr>
<td>debug dot1ag</td>
<td>Enable the tracing of CFM components for events and CFM PDUs based on the type of packet for reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug dot1x</td>
<td>Enables dot1x packet tracing.</td>
<td>PE</td>
</tr>
<tr>
<td>debug igmp snooping</td>
<td>Enables tracing of IGMP Snooping packets transmitted and/or received by the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip acl</td>
<td>Enables debug of IP Protocol packets matching the ACL criteria.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip bgp</td>
<td>Enables debug tracing of BGP events.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Traces DVMRP packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Traces IGMP packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip mcache</td>
<td>Traces MDATA packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip pimdm packet</td>
<td>Traces PIMDM packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ip pimsm packet</td>
<td>Traces PIMSM packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ipv6 dhcp</td>
<td>Displays debug information about DHCPv6 client activities and to trace DHCPv6 packets to and from the local DHCPv6 client.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ipv6 mcache</td>
<td>Traces MDATAv6 packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ipv6 mld</td>
<td>Traces MLD packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ipv6 pimdm</td>
<td>Traces PIMDMv6 packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ipv6 pimsm</td>
<td>Traces PIMSMv6 packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug isdp</td>
<td>Traces ISDP packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug lacp</td>
<td>Traces of LACP packets received and transmitted by the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>debug mldsnooping</td>
<td>Traces MLD snooping packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ospf</td>
<td>Enables tracing of OSPF packets received and transmitted by the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ospfv3</td>
<td>Enables tracing of OSPFv3 packets received and transmitted by the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>debug ping</td>
<td>Enables tracing of ICMP echo requests and responses.</td>
<td>PE</td>
</tr>
<tr>
<td>debug rip</td>
<td>Enables tracing of RIP requests and responses.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode^a</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>debug sflow</td>
<td>Enables sFlow debug packet trace.</td>
<td>PE</td>
</tr>
<tr>
<td>debug spanning-tree</td>
<td>Traces spanning tree BPDU packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug spanning-tree</td>
<td>Traces spanning tree BPDU packet reception and transmission.</td>
<td>PE</td>
</tr>
<tr>
<td>debug udld</td>
<td>Enables the display of UDLD packets or event processing.</td>
<td>PE</td>
</tr>
<tr>
<td>debug vpc</td>
<td>Enables debug traces for the specified protocols</td>
<td>GC</td>
</tr>
<tr>
<td>debug vrrp</td>
<td>Enables VRRP debug protocol messages.</td>
<td>PE</td>
</tr>
<tr>
<td>exception core-file</td>
<td>Configures the core dump file name.</td>
<td>GC</td>
</tr>
<tr>
<td>exception dump</td>
<td>Configures the core dump location.</td>
<td>GC</td>
</tr>
<tr>
<td>exception protocol</td>
<td>Enables full core dumps.</td>
<td>GC</td>
</tr>
<tr>
<td>exception switch-chip-register</td>
<td>Enables the dumping of the switch chip registers in case of an exception.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http timeout-policy</td>
<td>Configures the timeout policy for closing HTTP and HTTPS sessions to the local HTTP server.</td>
<td>GC</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays packet tracing configurations.</td>
<td>PE</td>
</tr>
<tr>
<td>show supported mibs</td>
<td>Displays the HTTP server status and configuration.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>show supported mibs</td>
<td>Displays the implemented SNMP MIBs.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>snapshot bgp</td>
<td>Dumps a set of BGP debug information to capture the current state of BGP.</td>
<td>S</td>
</tr>
<tr>
<td>write core</td>
<td>Generates a core file on demand and either, reboots the switch or tests the core file configuration.</td>
<td>PE</td>
</tr>
</tbody>
</table>

^a For the meaning of each Mode abbreviation, see Mode Types.
## sFlow

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow destination</td>
<td>Configures sFlow collector parameters (owner string, receiver timeout, ip address, and port).</td>
<td>GC</td>
</tr>
<tr>
<td>sflow polling</td>
<td>Enables a new sFlow poller instance for the data source if rcvr_idx is valid.</td>
<td>GC</td>
</tr>
<tr>
<td>sflow polling (Interface Mode)</td>
<td>Enable a new sFlow poller instance for this data source if rcvr_idx is valid.</td>
<td>IC</td>
</tr>
<tr>
<td>sflow sampling</td>
<td>Enables a new sFlow sampler instance for this data source if rcvr_idx is valid.</td>
<td>GC</td>
</tr>
<tr>
<td>sflow sampling (Interface Mode)</td>
<td>Enables a new sFlow sampler instance for this data source if rcvr_idx is valid.</td>
<td>IC</td>
</tr>
<tr>
<td>sflow source-interface</td>
<td>Selects the interface from which to use the IP address inserted in the source IP address field of transmitted sFlow packets.</td>
<td>GC</td>
</tr>
<tr>
<td>show sflow agent</td>
<td>Displays the sFlow agent information.</td>
<td>PE</td>
</tr>
<tr>
<td>show sflow destination</td>
<td>Displays all the configuration information related to the sFlow receivers.</td>
<td>PE</td>
</tr>
<tr>
<td>show sflow polling</td>
<td>Displays the sFlow polling instances created on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show sflow sampling</td>
<td>Displays the sFlow sampling instances created on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show sflow source-interface</td>
<td>Displays the assigned sFlow source interface.</td>
<td>PE or GC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

## SNMP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp</td>
<td>Displays the SNMP status.</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp engineid</td>
<td>Displays the SNMP engine ID.</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp filters</td>
<td>Displays the configuration of filters.</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp group</td>
<td>Displays the configuration of groups.</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode$^a$</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>show snmp user</td>
<td>Displays the configuration of users.</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp views</td>
<td>Displays the configuration of views.</td>
<td>PE</td>
</tr>
<tr>
<td>show trapflags</td>
<td>Displays SNMP traps globally or displays specific SNMP traps.</td>
<td>PE</td>
</tr>
<tr>
<td>snmp-server community</td>
<td>Sets up the community access string to permit access to SNMP protocol.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server community-</td>
<td>Maps SNMP v1 and v2 security models to the group name.</td>
<td>GC</td>
</tr>
<tr>
<td>group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>snmp-server contact</td>
<td>Sets up a system contact (sysContact) string.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>Enables SNMP traps globally or enables specific SNMP traps.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server engineID</td>
<td>Specifies the Simple Network Management Protocol (SNMP) engine ID on the</td>
<td>GC</td>
</tr>
<tr>
<td>local</td>
<td>local switch.</td>
<td></td>
</tr>
<tr>
<td>snmp-server filter</td>
<td>Creates or updates an SNMP server filter entry.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server group</td>
<td>Configures a new SNMP group or a table that maps SNMP users to SNMP views.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of SNMP notifications.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>Sets the system location string.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server user</td>
<td>Configures a new SNMP Version 3 user.</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server view</td>
<td>Creates or updates a Simple Network Management Protocol (SNMP) server view</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>entry.</td>
<td></td>
</tr>
<tr>
<td>snmp-server v3-host</td>
<td>Specifies the recipient of Simple Network Management Protocol Version 3</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>(SNMPv3) notifications.</td>
<td></td>
</tr>
<tr>
<td>snmp-server source-interface</td>
<td>Selects the interface from which to use the IP address in the source IP</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>address field of transmitted SNMP traps and informs.</td>
<td></td>
</tr>
</tbody>
</table>

$^a$ For the meaning of each Mode abbreviation, see Mode Types.
## Support Assist

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>eula-consent</td>
<td>Accepts or rejects the end-user license agreement (EULA) for the SupportAssist server.</td>
<td>GC</td>
</tr>
<tr>
<td>contact-company</td>
<td>Configures the contact information to be sent to the SupportAssist server.</td>
<td>SAC</td>
</tr>
<tr>
<td>contact-person</td>
<td>Configures the contact information to be sent to the SupportAssist server.</td>
<td>SAC</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a SupportAssist server.</td>
<td>SAC</td>
</tr>
<tr>
<td>proxy-ip-address</td>
<td>Configures a proxy server to be used to contact the SupportAssist servers.</td>
<td>SAC</td>
</tr>
<tr>
<td>server</td>
<td>Configures a SupportAssist server and enter SupportAssist server configuration mode.</td>
<td>SAC</td>
</tr>
<tr>
<td>show eula-consent</td>
<td>Reviews the EULA details whenever desired.</td>
<td>PE</td>
</tr>
<tr>
<td>show support-assist</td>
<td>Displays information on the SupportAssist feature status.</td>
<td>PE, GC</td>
</tr>
<tr>
<td>support-assist</td>
<td>Enables support-assist configuration mode if the EULA has been accepted.</td>
<td>GC</td>
</tr>
<tr>
<td>url</td>
<td>Configures the URL to reach on the SupportAssist remote server.</td>
<td>SAC</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see Mode Types.

## SYSLOG

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clears messages from the in memory logging buffer.</td>
<td>PE</td>
</tr>
<tr>
<td>clear logging file</td>
<td>Clears messages from the logging file.</td>
<td>PE</td>
</tr>
<tr>
<td>description (Logging)</td>
<td>Describes the SYSLOG server.</td>
<td>L</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the level of SYSLOG messages sent to the server.</td>
<td>L</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>logging cli-command</td>
<td>Enables CLI command logging.</td>
<td>GC</td>
</tr>
<tr>
<td>logging</td>
<td>Configures a SYSLOG server</td>
<td>GC</td>
</tr>
<tr>
<td>logging audit</td>
<td>Enables switch auditing.</td>
<td>GC</td>
</tr>
<tr>
<td>logging buffered</td>
<td>Enables logging to the in-memory log.</td>
<td>GC</td>
</tr>
<tr>
<td>logging console</td>
<td>Enables logging to the console.</td>
<td>GC</td>
</tr>
<tr>
<td>logging facility</td>
<td>Configures the facility to be used in SYSLOG messages.</td>
<td>GC</td>
</tr>
<tr>
<td>logging file</td>
<td>Enables logging to the persistent (on flash) log.</td>
<td>GC</td>
</tr>
<tr>
<td>logging monitor</td>
<td>Enables logging messages to telnet and SSH sessions with the default severity level.</td>
<td>GC</td>
</tr>
<tr>
<td>logging on</td>
<td>Enables error messages logging.</td>
<td>GC</td>
</tr>
<tr>
<td>logging protocol</td>
<td>Logs messages in RFC5424 of RFC 3164 format.</td>
<td>GC</td>
</tr>
<tr>
<td>logging snmp</td>
<td>Enables SNMP Set command logging.</td>
<td>GC</td>
</tr>
<tr>
<td>logging source-interface</td>
<td>Selects the interface from which to use the IP address in the source IP address field of transmitted SYSLOG packets.</td>
<td>GC</td>
</tr>
<tr>
<td>logging traps</td>
<td>Sets the lowest severity level at which SNMP traps are logged.</td>
<td>GC</td>
</tr>
<tr>
<td>logging web-session</td>
<td>Enables web session logging.</td>
<td>GC</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the port number on which the SYSLOG server listens for messages.</td>
<td>L</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of logging and the messages stored in the internal buffer.</td>
<td>PE</td>
</tr>
<tr>
<td>show logging file</td>
<td>Displays the state of logging and the messages stored in the logging file.</td>
<td>PE</td>
</tr>
<tr>
<td>show syslog-servers</td>
<td>Displays the SYSLOG server settings.</td>
<td>PE</td>
</tr>
<tr>
<td>terminal monitor</td>
<td>Enables the display of logging messages over a telnet of SSH session.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
## System Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset-tag</td>
<td>Specifies the switch asset-tag.</td>
<td>GC</td>
</tr>
<tr>
<td>banner exec</td>
<td>Sets the message that is displayed after a successful login.</td>
<td>GC</td>
</tr>
<tr>
<td>banner login</td>
<td>Sets the message that is displayed just before the login prompt.</td>
<td>GC</td>
</tr>
<tr>
<td>banner motd</td>
<td>Specifies message-of-the-day banner.</td>
<td>GC</td>
</tr>
<tr>
<td>banner motd acknowledge</td>
<td>Acknowledges message-of-the-day banner.</td>
<td>GC</td>
</tr>
<tr>
<td>buffers</td>
<td>Configures the rising and falling thresholds for the issuance of the message buffer SNMP trap and notification via a SYSLOG message.</td>
<td>GC</td>
</tr>
<tr>
<td>clear checkpoint statistics</td>
<td>Clears the statistics for the checkpointing process.</td>
<td>GC</td>
</tr>
<tr>
<td>clear counters stack-ports</td>
<td>Clears the statistics for all stack-ports.</td>
<td>PE</td>
</tr>
<tr>
<td>connect</td>
<td>Connects to the serial console of a different stack member.</td>
<td>PE</td>
</tr>
<tr>
<td>cut-through mode</td>
<td>Enables cut-through mode on the switch (if supported).</td>
<td>GC</td>
</tr>
<tr>
<td>exit</td>
<td>Disconnects the serial connection to the remote unit.</td>
<td>UE</td>
</tr>
<tr>
<td>hardware profile portmode</td>
<td>Configures a 40G port in 4x10G mode or 1x40G mode.</td>
<td>IC</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies or modifies the switch host name.</td>
<td>GC</td>
</tr>
<tr>
<td>initiate failover</td>
<td>Forces failover of management unit.</td>
<td>GC</td>
</tr>
<tr>
<td>load-interval</td>
<td>Loads the interface utilization measurement interval.</td>
<td>IC</td>
</tr>
<tr>
<td>locate</td>
<td>Locates a switch by LED blinking.</td>
<td>PE</td>
</tr>
<tr>
<td>logout</td>
<td>Disconnects the serial connection to a remote unit on a stack member.</td>
<td>UE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>member</td>
<td>Preconfigures a stack member.</td>
<td>SG</td>
</tr>
<tr>
<td>memory free low-watermark</td>
<td>Configures the notification of a low memory condition on the switch for the issuance of the CPU overload SNMP trap and notification via a SYSLOG message.</td>
<td>GC</td>
</tr>
<tr>
<td>nsf</td>
<td>Specifies non-stop forwarding.</td>
<td>GC</td>
</tr>
<tr>
<td>ping</td>
<td>Sends ICMP echo request packets to another node on the network.</td>
<td>UE</td>
</tr>
<tr>
<td>process cpu threshold</td>
<td>Configures the rising and falling thresholds for the issuance of the CPU overload SNMP trap and notification via a SYSLOG message.</td>
<td>GC</td>
</tr>
<tr>
<td>quit</td>
<td>Disconnects the serial connection to the remote unit on a stack member.</td>
<td>UE</td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
<td>PE</td>
</tr>
<tr>
<td>set description</td>
<td>Associates a text description with a switch in the stack.</td>
<td>SG</td>
</tr>
<tr>
<td>slot</td>
<td>Configures a slot in the system.</td>
<td>GC</td>
</tr>
<tr>
<td>show banner</td>
<td>Displays banner information.</td>
<td>PE</td>
</tr>
<tr>
<td>show buffers</td>
<td>Displays the system allocated buffers.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show checkpoint statistics</td>
<td>Displays the statistics for the checkpointing process.</td>
<td>PE</td>
</tr>
<tr>
<td>show cut-through mode</td>
<td>Show the cut-through mode on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show hardware profile</td>
<td>Displays the hardware profile information for the 40G ports.</td>
<td>PE</td>
</tr>
<tr>
<td>show idprom interface</td>
<td>Displays the optics EEPROM contents in a user-readable format.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the traffic statistics for one or multiple interfaces.</td>
<td>UE</td>
</tr>
<tr>
<td>show interfaces advanced firmware</td>
<td>Displays the firmware revision of the PHY for a port.</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the static and dynamic parameters for the optics.</td>
<td>UE or PE</td>
</tr>
</tbody>
</table>

<sup>a</sup> Mode: SG = Stack Group, GC = Global Control, UE = User EXEC, PE = Privileged EXEC
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces utilization</td>
<td>Displays the interface utilization.</td>
<td>PE</td>
</tr>
<tr>
<td>show memory cpu</td>
<td>Checks the total and available RAM space on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show nsf</td>
<td>Shows non-stop forwarding status.</td>
<td>PE</td>
</tr>
<tr>
<td>show power-usage-history</td>
<td>Shows the history of unit power consumption for the unit specified in the command and total stack power consumption.</td>
<td>PE</td>
</tr>
<tr>
<td>show process app-list</td>
<td>Displays the system applications.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show process app-resource-list</td>
<td>Lists the configured and in-use resources for each application known to the Process Manager.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show process cpu</td>
<td>Checks the CPU utilization for each process currently running on the switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show process proc-list</td>
<td>Lists the configured and in-use resources for each application known to the Process Manager.</td>
<td>PE or GC</td>
</tr>
<tr>
<td>show sessions</td>
<td>Displays a list of the open console sessions.</td>
<td>PE</td>
</tr>
<tr>
<td>show slot</td>
<td>Displays information about all the slots in the system or for a specific slot.</td>
<td>UE</td>
</tr>
<tr>
<td>show supported cardtype</td>
<td>Displays information about all card types supported in the system.</td>
<td>UE</td>
</tr>
<tr>
<td>show supported switchtype</td>
<td>Displays information about all supported switch types.</td>
<td>UE</td>
</tr>
<tr>
<td>show switch</td>
<td>Displays information about the switch status.</td>
<td>UE</td>
</tr>
<tr>
<td>show system</td>
<td>Displays system information.</td>
<td>UE</td>
</tr>
<tr>
<td>show system fan</td>
<td>Explicitly displays the fan status.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show system id</td>
<td>Displays the service ID information.</td>
<td>UE</td>
</tr>
<tr>
<td>show system power</td>
<td>Displays information about the system level power consumption.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show system temperature</td>
<td>Displays information about the system temperature and fan status.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>show tech-support</td>
<td>Displays system and configuration information (for debugging/calls to technical support).</td>
<td>PE</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show users</td>
<td>Displays information about the active users, including which profiles have been assigned to local user accounts and which profiles are active for logged-in users.</td>
<td>PE</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the system version information.</td>
<td>UE</td>
</tr>
<tr>
<td>stack</td>
<td>Sets the mode to Stack Configuration mode.</td>
<td>GC</td>
</tr>
<tr>
<td>stack-port</td>
<td>Sets the mode to Stack Configuration mode to configure Stack ports as either Stacking ports or as Ethernet ports.</td>
<td>GC</td>
</tr>
<tr>
<td>stack-port shutdown</td>
<td>Enables or disable the stack port administratively.</td>
<td>SC</td>
</tr>
<tr>
<td>standby</td>
<td>Configures the standby in the stack.</td>
<td>SG</td>
</tr>
<tr>
<td>switch renumber</td>
<td>Changes the identifier for a switch in the stack.</td>
<td>GC</td>
</tr>
<tr>
<td>telnet</td>
<td>Logs into a host that supports Telnet.</td>
<td>PE</td>
</tr>
<tr>
<td>traceroute</td>
<td>Discovers the IP routes that packets actually take when traveling to their destinations.</td>
<td>PE</td>
</tr>
<tr>
<td>traceroute ipv6</td>
<td>Discovers the IP routes that packets actually take when traveling to their destinations.</td>
<td>PE</td>
</tr>
<tr>
<td>update bootcode</td>
<td>Updates the boot code on one or more switches.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.

**Telnet Server**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip telnet server disable</td>
<td>Enables/disables the Telnet service on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>ip telnet port</td>
<td>Configures the Telnet TCP port number on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>show ip telnet</td>
<td>Displays the status of the Telnet server and the Telnet TCP port number.</td>
<td>PE</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
## Time Ranges

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>time-range [name]</td>
<td>Creates a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries.</td>
<td>GC</td>
</tr>
<tr>
<td>absolute</td>
<td>Adds an absolute time entry to a time range.</td>
<td>TRC</td>
</tr>
<tr>
<td>periodic</td>
<td>Adds a periodic time entry to a time range.</td>
<td>TRC</td>
</tr>
<tr>
<td>show time-range</td>
<td>Displays a time range and all the absolute/periodic time entries that are defined for the time range.</td>
<td>PE</td>
</tr>
</tbody>
</table>

¹ For the meaning of each Mode abbreviation, see Mode Types.

## USB Flash Drive

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>unmount usb</td>
<td>Makes the USB flash device inactive.</td>
<td>PE</td>
</tr>
<tr>
<td>show usb</td>
<td>Displays the USB flash device details.</td>
<td>PE</td>
</tr>
<tr>
<td>dir usb</td>
<td>Displays the USB device contents and memory statistics.</td>
<td>PE</td>
</tr>
<tr>
<td>recover</td>
<td>Mounts the USB stick, copies the image from the USB root level directory into RAM, and executes the image.</td>
<td>UB</td>
</tr>
</tbody>
</table>

¹ For the meaning of each Mode abbreviation, see Mode Types.

## User Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters Global Configuration mode.</td>
<td>PE</td>
</tr>
<tr>
<td>do</td>
<td>Executes commands available in Privileged Exec mode with command line completion.</td>
<td>All except PE and UE</td>
</tr>
<tr>
<td>enable</td>
<td>Enters the privileged Exec mode.</td>
<td>UE</td>
</tr>
</tbody>
</table>
### Dell EMC Networking CLI

#### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Gets the CLI user control back to the privileged execution mode or user execution mode.</td>
<td>Any</td>
</tr>
<tr>
<td>exit</td>
<td>Exits any configuration mode to the previously highest mode in the CLI mode hierarchy.</td>
<td>(All)</td>
</tr>
<tr>
<td>quit</td>
<td>exit</td>
<td>logout</td>
</tr>
</tbody>
</table>

<sup>a</sup> For the meaning of each Mode abbreviation, see **Mode Types**.

#### Web Server

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Mode&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-name</td>
<td>Specifies the common-name for the device.</td>
<td>CC</td>
</tr>
<tr>
<td>country</td>
<td>Specifies the country.</td>
<td>CC</td>
</tr>
<tr>
<td>crypto certificate generate</td>
<td>Generates a HTTPS certificate.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto certificate import</td>
<td>Imports a certificate signed by the Certification Authority for HTTPS.</td>
<td>GC</td>
</tr>
<tr>
<td>crypto certificate request</td>
<td>Generates and displays a certificate request for HTTPS.</td>
<td>PE</td>
</tr>
<tr>
<td>duration</td>
<td>Specifies the duration in days.</td>
<td>CC</td>
</tr>
<tr>
<td>ip http port</td>
<td>Specifies the TCP port for use by a web browser to configure the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http server</td>
<td>Enables the switch to be configured from a browser.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http secure-certificate</td>
<td>Configures the active certificate for HTTPS.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http secure-port</td>
<td>Configures a TCP port for use by a secure web browser to configure the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>ip http secure-server</td>
<td>Enables the switch to be configured, monitored, or modified securely from a browser.</td>
<td>GC</td>
</tr>
<tr>
<td>key-generate</td>
<td>Specifies the key-generate.</td>
<td>CC</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the location or city name.</td>
<td>CC</td>
</tr>
<tr>
<td>no crypto certificate</td>
<td>Deletes a certificate from the switch.</td>
<td>GC</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode$^a$</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>organization-unit</td>
<td>Specifies the organization-unit or department name.</td>
<td>CC</td>
</tr>
<tr>
<td>show crypto certificate mycertificate</td>
<td>Displays the SSL certificates of your switch.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip http server status</td>
<td>Displays the HTTP server status information.</td>
<td>PE</td>
</tr>
<tr>
<td>show ip http server secure status</td>
<td>Displays the HTTP secure server status information.</td>
<td>UE or PE</td>
</tr>
<tr>
<td>state</td>
<td>Specifies the state or province name.</td>
<td>CC</td>
</tr>
</tbody>
</table>

a. For the meaning of each Mode abbreviation, see Mode Types.
Using the CLI

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Introduction

This section describes the basics of entering and editing the Dell EMC Networking N1100-ON, N1500, N2000, N2100-ON, N3000, N3000-ON, N3100-ON, and N4000 Series Command Line Interface (CLI) commands and defines the command hierarchy. It also explains how to activate the CLI and implement its major functions.

This section covers the following topics:

- Entering and Editing CLI Commands
- CLI Command Modes
- Starting the CLI
- Using CLI Functions and Tools

Entering and Editing CLI Commands

A CLI command is a series of keywords and arguments. The total number of characters that may be entered in a single command is limited to 1536 characters. Keywords identify a command and arguments specify configuration parameters. For example, in the command `show interfaces status gigabitethernet 1/0/5`, `show`, `interfaces` and `status` are keywords; `gigabitethernet` is an argument that specifies the interface type, and `1/0/5` is an argument that specifies the unit/slot/port.

When working with the CLI, the command options are not displayed. The command is not selected by a menu but is entered manually. To see what commands are available in each mode or within an Interface Configuration, the CLI provides a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request context-sensitive help is the `<?>` key.
Two instances where the help information can be displayed are:

- **Keyword lookup** — The `<?>` key is entered in place of a command. A list of all valid commands and corresponding help messages is displayed.

- **Partial keyword lookup** — A command is incomplete and the `<?>` key is entered in place of a parameter. The matched parameters for this command are displayed.

The following features and conventions are applicable to CLI command entry and editing:

- History Buffer
- Negating Commands
- Show Command
- Command Completion
- Short Form Commands
- Keyboard Shortcuts
- Command line parameters are entered by the user to choose an individual value or range of values for the specific command. Command line parameters are not syntax or range checked until the carriage return is entered. In some cases, the user may need to enter special characters, most often in a string parameter such as a password or a label. Special characters are one of the following characters (`! $ % ^ & * ( ) _ - + = { [ ] } : ; @ ' " ~ # | \ < , > . / ) or a blank. In these cases, it may be necessary to enclose the entire string in double or single quotes for the command line parser to properly interpret the parameter.

- Parameters
- Command Scripting
- CLI Command Notation Conventions
- Interface Naming Conventions

**History Buffer**

Every time a command is entered in the CLI, it is recorded in an internally managed Command History buffer. Commands are stored in the buffer, which operates on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved after switch resets.
By default, the history buffer system is enabled, but it can be disabled at any time. The standard number of 10 stored commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see the history size command in the Line command mode section of this guide.

### Negating Commands
For many commands, the prefix keyword no is entered to cancel the effect of a command or reset the configuration to the default value. Nearly all configuration commands have this capability. This guide describes the negation effect for all commands to which it applies.

### Show Command
The show command executes in the User Executive (Exec), Privileged Executive (Exec), Global Configuration mode, Interface Configuration mode and all configuration submodes with command completion. Output from show commands is paginated. Use the terminal length command to set the number of lines displayed in a page. When the paging prompt appears, press the space bar to display the next page of output or the enter key to display the next line of output.

**Example:**
```
console>en
console#configure
```
console(config)#interface Gi1/0/1
console(config-if-Gi1/0/1)#show interface status

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Link</th>
<th>Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td></td>
<td>N/A</td>
<td>Unknown Auto</td>
<td>Down</td>
<td>Inactive</td>
<td></td>
</tr>
</tbody>
</table>

**Command Completion**

CLI can complete partially entered commands when the user presses the <tab> or <space> key. If a command entered is not complete, is not valid, or if some parameters of the command are not valid or missing, an error message is displayed to assist in entering the correct command. By pressing the <tab> key, an incomplete command is changed into a complete command. If the characters already entered are not enough for the system to identify a single matching command, the <?> key displays the available commands matching the characters already entered.

**Short Form Commands**

The CLI supports the short forms of all commands. As long as it is possible to recognize the entered command unambiguously, the CLI accepts the short form of the command as if the user typed the full command.

**Keyboard Shortcuts**

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The help command, when used in the User Exec and Privileged Exec modes, displays the keyboard shortcuts.

Table 2-2 contains the CLI shortcuts displayed by the help command.
Table 2-2. CLI Shortcuts

<table>
<thead>
<tr>
<th>Keyboard Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Delete, Backspace&gt;</td>
<td>Delete previous character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;A&gt;</td>
<td>Go to beginning of line</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;E&gt;</td>
<td>Go to end of line</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;F&gt;</td>
<td>Go forward one character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;B&gt;</td>
<td>Go backward one character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;D&gt;</td>
<td>Delete current character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;U,X&gt;</td>
<td>Delete to beginning of line</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;K&gt;</td>
<td>Delete to the end of the line.</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;W&gt;</td>
<td>Delete previous word</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;T&gt;</td>
<td>Transpose previous character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;P&gt;</td>
<td>Go to previous line history buffer</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;R&gt;</td>
<td>Rewrites or pastes the line</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;N&gt;</td>
<td>Go to next line in history buffer</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;Y&gt;</td>
<td>Print last deleted character</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;Q&gt;</td>
<td>Pauses screen output.</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;S&gt;</td>
<td>Resumes screen output.</td>
</tr>
<tr>
<td>&lt;Ctrl&gt;+&lt;Z&gt;</td>
<td>Return to root command prompt</td>
</tr>
<tr>
<td>&lt;Tab, SPACE&gt;</td>
<td>Command-line completion</td>
</tr>
<tr>
<td>end</td>
<td>Return to the root command prompt</td>
</tr>
<tr>
<td>exit</td>
<td>Go to next lower command prompt</td>
</tr>
<tr>
<td>&lt;*&gt;</td>
<td>List choices</td>
</tr>
</tbody>
</table>

**Parameters**

Command line parameters are entered by the user to choose an individual value or range of values for the specific command. Command line parameters are not syntax or range checked until the carriage return is entered. In some cases, the user may need to enter special characters, most often in a string parameter such as a password or a label. Special characters are one of the following characters (`! $ % ^ & * ( ) _ - + = { [ } ] ; @ " ~ # | \ < , > ./`)
) or a blank. In these cases, it may be necessary to enclose the entire string in double or single quotes for the command line parser to properly interpret the parameter.

**Command Scripting**

The CLI can be used as a programmable management interface. To facilitate this function, any characters entered after the <!> character are treated as a comment and ignored by the CLI. Also, the CLI allows the user to disable session timeouts.

**CLI Command Notation Conventions**

When entering commands there are certain command-entry notations which apply to all commands. Table 2-3 describes these conventions as they are used in syntax definitions.
Table 2-3. CLI Command Notation Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>In a command line, square brackets indicate an optional entry.</td>
</tr>
<tr>
<td>{ }</td>
<td>In a command line inclusive brackets indicate a selection of compulsory parameters separated by the</td>
</tr>
</tbody>
</table>

Italic Indicates a variable.

<Enter> Any individual key on the keyboard.

<Ctrl>+<F4> Any combination of keys pressed simultaneously on the keyboard.

Screen Display Indicates system messages and prompts appearing on the console.

all Indicates a literal parameter, entered into the command as it is.

Interface Naming Conventions

The conventions for naming interfaces in CLI commands are as follows:

Ethernet Interfaces

Individual Ethernet interfaces (Gigabit Ethernet, Ten Gigabit Ethernet, and Forty Gigabit Ethernet) are identified in the CLI by the variable unit/slot/port, where:

- `<Interface Type> Unit#/Slot#/Port# — Identifies a specific interface by the interface type tag followed by the Unit# followed by a / symbol, then the Slot# followed by a / symbol, and then the Port#. For example, gi2/0/10 identifies the Gigabit interface 10 in slot 0 within the second unit on a non-blade switch. Table 2-4 below lists the supported interface type tags.

- Unit # — The unit number is greater than 1 only in a stacking solution where a number of switches are stacked to form a virtual switch. In this case, the Unit# indicates the logical position of the switch in a stack. The range is 1–12. The unit value is 1 for standalone switches.
• **Slot#** — The slot number is an integer number assigned to a particular slot. Front panel ports have a slot number of 0. Rear panel ports are numbered from 1 and can be identified by the lexan on the rear panel. Use the `show slot` command to retrieve information for a particular slot.

• **Port #** — The port number is an integer number assigned to the physical port on the switch and corresponds to the lexan printed next to the port on the front or back panel. Ports are numbered from 1 to the maximum number of ports available on the switch unit, typically 24 or 48.

Logical interfaces are identified by one of the keywords: loopback, port-channel, tunnel or vlan followed an integer index identifying the specific logical interface.

Within this document, unless specified otherwise, the tag interface–id refers to a logical or Ethernet interface identifier that follows the naming convention above. If the command is restricted to a subset of the interfaces, then the subset is described in the command description. Ethernet interfaces are Gigabitethernet, Tengigabitethernet, and Fortygigabitethernet. NBASE-T interfaces running at 2.5 and 5 Gigabit speeds are identified as Gigabitethernet.
Table 2-4. Interface Identifiers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Long Form</th>
<th>Short Form</th>
<th>Single Character Short Form</th>
<th>Interface Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>Gigabitethernet</td>
<td>G or Gi</td>
<td>Y</td>
<td>unit/slot/port</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>Tengigabitethernet</td>
<td>Te</td>
<td>Y</td>
<td>unit/slot/port</td>
</tr>
<tr>
<td>21-Gigabit Stacking</td>
<td>Twentygigabitstacking</td>
<td>Tw</td>
<td>n/a</td>
<td>unit/slot/port</td>
</tr>
<tr>
<td>40-Gigabit Ethernet</td>
<td>Fortygigabitethernet</td>
<td>Fo</td>
<td>Y</td>
<td>unit/slot/port</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback</td>
<td>Lo</td>
<td>Y</td>
<td>loopback-id (0-7)</td>
</tr>
<tr>
<td>Port Channel</td>
<td>Port-channel</td>
<td>Po</td>
<td>Y</td>
<td>port-channel-number (1-128) N1500 (1–64)</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel</td>
<td>Tu</td>
<td>n/a</td>
<td>tunnel-id (0-7)</td>
</tr>
<tr>
<td>Vlan</td>
<td>VLAN</td>
<td>Vl</td>
<td>Y</td>
<td>vlan-id (1-4093)</td>
</tr>
</tbody>
</table>

A single character short form of the interface commands indicated in Table 2-4 is implemented in version 6.5 for Gigabit Ethernet interfaces only.

When listed in command line output, Gigabit Ethernet interfaces are preceded by the characters Gi, Ten-Gigabit Ethernet interfaces are preceded by Te, and Forty-Gigabit Ethernet interfaces are preceded by Fo, as shown in the examples below.

**Stacking Interfaces**

Stacking interfaces are represented in the CLI with the same unit/slot/port form as Ethernet interfaces. The fixed stacking interfaces on the N2000/N2100-ON/N3000 switches always use the TwentyGigabitStacking or Tw notation and on the N1100-ON/N1500/N4000 switches, are referred to using Ethernet notation.
Loopback Interfaces

Loopback interfaces are represented in the CLI by the keyword `loopback` followed by the variable `loopback-id`, which can assume values from 0–7.

Port Channel Interfaces

Port-channel (or LAG) interfaces are represented in the CLI by the keyword `port-channel` followed by the variable `port-channel-number`. When listed in command line output, port channel interfaces are preceded by the characters Po.

Tunnel Interfaces

Tunnel interfaces are represented in the CLI by the keyword `tunnel` followed by the variable `tunnel-id`, which can assume values from 0–7.

VLAN Routing Interfaces

VLAN interfaces are represented in the CLI by the keywords `interface vlan` followed by the variable `vlan-id`, which can assume values from 1-4093. A VLAN routing interface will typically have an IP address assigned, either via DHCP or a static assignment or, in the case of IPv6, auto assignment of a link local address.

Operating on Multiple Interfaces (Ranges)

The CLI allows the user to operate on multiple interfaces in one operation. The guidelines are as follows for range operation:

- The `range` key word is used to identify that an interface range specifier follows.
  - An interface range specifier consists of an interface identifier followed by an optional range parameter. The interface type may be an Ethernet interface or a logical interface (port channel or VLAN) as described in the Interface Naming Conventions section.

- The range parameter may be written in the following manner:
  - (#-#) — a range from a particular interface to another higher-numbered interface (inclusive). For example, 1/0/1-10 indicates that the operation applies to the Ethernet interfaces 1 to 10 in slot 0 on unit 1. The number
to the left of the hyphen must always be less than or equal to the number to the right of the hyphen, e.g. interface range Gi1/0/10-1 is not valid.

(#, #, #) — a list of interfaces. For example, (1/0/1, 1/0/1,1/0/3, 1/0/5) indicates that the operation applies to the Ethernet interfaces 1, 3, and 5 on unit 1. The interfaces may or may not be consecutive, nor must the interfaces be of the same type.

(#, #-#, #) — ranges and non-consecutive interfaces listed together. For example, (1/0/1, 1/0/3-5, 1/0/7) indicates that the operation applies to the Ethernet interfaces 1, 3, 4, 5, and 7 on unit 1.

**NOTE:** Each Ethernet interface must be a fully qualified interface identifier in the format unit/slot/port. See Interface Naming Conventions.

- Port channels and VLANs are supported in ranges.
- No spaces are allowed anywhere in a range parameter, e.g. Gi1/0/1 -2 is not accepted, nor is Gi1/0/2, Gi1/0/4. Use Gi1/0/1-2 and Gi/1/0/2,Gi1/0/4 respectively.
- When operating on a range of interfaces, the CLI implementation hides the parameters that may not be configured in a range (for example, parameters that must be uniquely configured for each instance).
- The CLI uses best effort when operating on a list of objects. If the user requests an operation on a list of objects, the CLI attempts to execute the operation on as many objects in the list as possible even if failure occurs for some of the items in the list. The CLI provides the user with a detailed list of all failures, listing the objects and the reasons for the failures.

Some parameters must be configured individually for each port or interface.

**Examples**

Example 1 shows the various forms of interface notation that can be entered in the CLI. Examples 2 and 3 show various forms of CLI output using shorthand interface notation.

**Example #1**

```
  gigabitethernet 1/0/1
  gigabitethernet1/0/1 (there is no space)
  gi 1/0/1
  gi1/0/1 (there is no space)
  port-channel 1
  vlan 5
```
Example #2

console(config-if-Gi1/0/23)#show vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>Po1-128, Gi1/0/1-24, Tel0/1-2</td>
<td>Default</td>
</tr>
</tbody>
</table>

RSPAN Vlan

None

console(config-if-Gi1/0/23)#show slot 2/0

Slot.............................. 2/0
Slot Status....................... Empty
Admin State....................... Enable
Power State....................... Enable
Configured Card:
  Model Identifier............... Dell Networking N3024F
  Card Description............... Dell 24 Port 10G Fiber
  Pluggable......................... No

Example #3

console(config-if-Gi1/0/23)#show slot

<table>
<thead>
<tr>
<th>Slot</th>
<th>Admin Status</th>
<th>Power Status</th>
<th>Configured Card</th>
<th>Pluggable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0</td>
<td>Full</td>
<td>Enable</td>
<td>Dell Networking N3024F</td>
<td>No</td>
</tr>
<tr>
<td>1/1</td>
<td>Empty</td>
<td>Disable</td>
<td>Disable</td>
<td>Yes</td>
</tr>
<tr>
<td>2/0</td>
<td>Empty</td>
<td>Enable</td>
<td>Dell Networking N3024F</td>
<td>No</td>
</tr>
<tr>
<td>2/1</td>
<td>Empty</td>
<td>Enable</td>
<td>Dell Networking N3024F</td>
<td>Yes</td>
</tr>
<tr>
<td>3/0</td>
<td>Empty</td>
<td>Enable</td>
<td>Dell Networking N3048</td>
<td>No</td>
</tr>
<tr>
<td>3/1</td>
<td>Empty</td>
<td>Enable</td>
<td>Dell Networking N3048</td>
<td>Yes</td>
</tr>
</tbody>
</table>

console(config-if-Gi1/0/23)#show slot 1/0

Slot.............................. 1/0
Slot Status........................ Full
Admin State....................... Enable
Power State....................... Enable
Inserted Card:
  Model Identifier............... Dell Networking N3024F
Card Description.................. Dell 24 Port 10G Fiber
Configured Card:
  Model Identifier............... Dell Networking N3024F
  Card Description............... Dell 24 Port 10G Fiber
Pluggable.......................... No

**Entering Network Addresses**

**MAC Addresses**

MAC addresses are specified in 3 groups of four upper or lower case hexadecimal characters separated by periods with no spaces, e.g. 0011.2233.FFee or by eight pairs of upper or lower case hexadecimal characters separated by colons, e.g. 00:11:22:33:FF:ee. Leading zeros must be specified in all cases.

**IPv4 Addresses**

IPv4 addresses are specified by four groups of decimal integers in the range 0-255, i.e. dotted quad notation. Leading zeros are not required. Example IPv4 addresses are 1.2.3.4 or 255.255.255.255.

The net mask, if specified, consists of four decimal digits in dotted quad notation, e.g. 255.255.252.0 or a decimal prefix length preceded by a forward slash and indicating the number of left justified 1 bits in the net mask. The net mask is always separated from an IPv4 address by one or more spaces, regardless of the format. Bits that are not significant must be zeroed, for example, 1.1.1.1/24 is not a valid subnet as the rightmost 1 bit is not configured to be a zero. User 1.1.1.0/24 instead.

**Examples:**

1.2.3.0 /24 is equivalent to 1.2.3.0 255.255.255.0

**IPv6 Addresses**

IPv6 addresses may be expressed in up to eight blocks of four upper or lower case hexadecimal characters. For simplification, the leading zeros of each 16 bit block may be omitted. One sequence of 16 bit blocks - containing only zeros - may be replaced by a double colon”::”, but not more than one at a time. Example IPv6 addresses are:

Dropped zeros: 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1
Local Host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The prefix length, if specified, ranges from 1 to 128 and is specified by a forward slash and a decimal number indicating the significant bits of the address, e.g. 3ffe:ffff:100:f101:0:0:0:/64. No spaces are allowed between the last address digit or colon and the forward slash.
CLI Command Modes

Since the set of CLI commands is very large, the CLI is structured as a command-tree hierarchy, where related command sets are assigned to command modes for easier access. At each level, only the commands related to that level are available to the user and only those commands are shown in the context sensitive help for that level.

In this guide, commands are organized into multiple categories:

- Layer 2 Switching commands
- Security commands
- Audio Visual Bridging commands
- Data Center Technology commands
- Layer 3 Routing commands
- Switch Management commands

Layer 2 Switching describes the commands used for filtering and forwarding of packets within a VLAN based upon learned MAC addresses.

Security describes the commands used to configure switch administrator and end user network access.

Audio Visual Bridging describes the commands utilized to configure IEEE 802.1BA systems.

Data Center Technology describes the commands used to configure ANSI T11 FC-BB-5 and OpenFlow capabilities.

Layer 3 Routing describes the commands used to forward packets within and across VLANs based upon the IP addresses as well as management of the routing protocols necessary to enable the distribution of routes.

Switch Management describes commands used to manage the switch.

Commands that cause specific actions to be taken immediately by the system and do not directly affect the system configurations are defined at the top of the command tree. For example, commands for rebooting the system or for downloading or backing up the system configuration files are placed at the top of the hierarchy tree.

Commands that result in configuration changes to the switch are grouped in a Global Configuration sub tree.
There are levels beneath the Global Configuration mode for further grouping of commands. The system prompt reflects these sub-Configuration modes. All the parameters are provided with reasonable defaults where possible.

When starting a session, the initial mode is the User Exec mode (privilege level 0). Only a limited subset of commands is available in this mode. This level is reserved for tasks that do not change the configuration. To enter the next level, Privileged Exec mode (privilege level 1) may be required if configured by the administrator.

Privileged Exec mode provides access to commands that can not be executed in the User Exec mode and permits access to Global Configuration mode.

Global Configuration mode manages switch configuration on a global level. For specific configurations, command modes exist at a sublevel.

Entering a <???> at the system prompt displays a list of commands available for that particular command mode. A specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: User Exec mode, Privileged Exec mode, Global Configuration mode, and Interface Configuration and other specific configuration modes.

**User Exec Mode**

After logging into the switch, the user is automatically in the User Exec command mode unless the user is defined as a privileged user. In general, the User Exec commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the switch host name followed by the angle bracket (>).

```
Console>
```

The default host name is Console unless it has been changed using the `hostname` command in Global Configuration mode.

**Privileged Exec Mode**

Because many of the privileged commands set operating parameters, privileged access may be password-protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive.

Privileged users enter into the Privileged Exec mode from User Exec mode, where the following prompt is displayed.
Global Configuration Mode

Global Configuration commands allow the operator to change the configuration of the switch. The Privileged Exec mode command `configure` (or `configure terminal`) is used to enter Global Configuration mode.

console(config)#

The following are the Global Configuration submodes:

- **SNMP v3 Host Configuration** — Configures the parameters for the SNMP v3 server host.
- **SNMP Community Configuration** — Configures the parameters for the SNMP server community.
- **MST** — The Global Configuration mode command spanning-tree mst configuration is used to enter into the Multiple Spanning Tree configuration mode.
- **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed and time-out settings. The Global Configuration mode command `line` is used to enter the Line Interface mode.
- **Router OSPF Configuration** — Global configuration mode command `router ospf` is used to enter into the Router OSPF Configuration mode.
- **Router RIP Configuration** — Global configuration mode command `router rip` is used to enter into the Router RIP Configuration mode.
- **Router OSPFv3 Configuration** — Global configuration mode command `ipv6 router ospf` is used to enter into the Router OSPFv3 Configuration mode.
- **Router BGP Configuration** — Global configuration mode command `router bgp` is used to enter into the Router BGP Configuration mode.
- **IPv6 DHCP Pool Mode** — Global configuration mode command `ipv6 dhcp pool` is used to enter into the IPv6 DHCP Pool mode.
- **Management Access List** — Contains commands to define management access administration lists. The Global Configuration mode command `management access-list` is used to enter the Management Access List configuration mode.
• **Policy-map** — Use the `policy-map` command to access the QoS policy map configuration mode to configure the QoS policy map.

• **Policy Class** — Use the `class` command to access the QoS Policy-class mode to attach or remove a diffserv class from a policy and to configure the QoS policy class.

• **Class-Map** — This mode consists of class creation/deletion and matching commands. The class matching commands specify layer 2, layer 3 and general match criteria. Use the `class-map class-map-name` commands to access the QoS Class Map Configuration mode to configure QoS class maps.

• **Stack** — Use the stack command to access the Stack Configuration Mode.

• **SSH Public Key-chain** — Contains commands to manually specify other switch SSH public keys. The Global Configuration mode command `crypto key pub-key chain ssh` is used to enter the SSH Public Key-chain configuration mode.

• **SSH Public Key-string** — Contains commands to manually specify the SSH Public-key of a remote SSH Client.

• **MAC Access-List** — Configures conditions required to allow traffic based on MAC addresses. The Global Configuration mode command `mac access-list` is used to enter the MAC Access-List configuration mode.

• **TACACS** — Configures the parameters for the TACACS server.

• **RADIUS** — Configures the parameters for the RADIUS server.

• **SNMP Host Configuration** — Configures the parameters for the SNMP server host. Only IPv4 hosts are supported.

• **Crypto Certificate Request** — Configures the parameters for crypto certificate request.

• **Crypto Certificate Generation** — Configures the parameters for crypto certificate generate.

• **Logging** — Configures the parameters for SYSLOG servers.

• **VLAN** — Creates a VLAN and configures non-L3 parameters on a VLAN.

• **Virtual Router Configuration** — Configures parameters for a virtual routing instance.
Pre-configuration

Nearly all switch features support a pre-configuration capability, even when a feature is not enabled or the required hardware is not present. Pre-configured capabilities become active only when enabled (typically via an admin mode control) or when the required hardware is present (or both). For example, a port can be pre-configured with both trunk and access mode information. The trunk mode information is applied only when the port is placed into trunk mode and the access mode information is only applied when the port is placed into access mode. Likewise, OSPF routing can be configured in the switch without being enabled on any port.

Interface Configuration Modes

Interface configuration modes are used to modify specific interface operations. The following are the Interface Configuration and other specific configuration modes:

- **Ethernet** — Contains commands to manage Ethernet port configuration. The Global Configuration mode command `interface interface-id` enters the Interface Configuration mode to configure an Ethernet interface.

- **Port Channel** — Contains commands to configure port-channels, i.e., assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode and are used to manage the member ports as a single entity. The Global Configuration mode command `interface port-channel port-channel-number` is used to enter the Port Channel mode.

- **Tunnel** — Contains commands to manage tunnel interfaces. The Global Configuration mode command `interface tunnel` enters the Tunnel Configuration mode to configure a tunnel type interface.

- **Loopback** — Contains commands to manage loopback interfaces. The Global Configuration mode command `interface loopback` enters the Loopback Configuration mode to configure an loopback type interface.

- **Out-of-band**—Contains commands to manage the out-of-band interface, if present. The Global Configuration mode command `interface out-of-band` enters the Out-of-band Interface mode to configure the out-of-band interface.
• **Interface VLAN**— Enables routing on a VLAN and configures routing/L3 parameters on a VLAN.

**Identifying the Switch and Command Mode from the System Prompt**

The system prompt provides the user with the name of the switch (hostname) and identifies the command mode. The following is a formal description of the system command prompt:

```
[device name][[[command mode-[object]]]][# | >]
```

[device name] — is the name of the managed switch, which is typically the user-configured hostname established by the `hostname` command.

[command mode] — is the current configuration mode and is omitted for the top configuration levels.

[object] — indicates specific object or range of objects within the configuration mode.

For example, if the current configuration mode is config-if and the object being operated on is Gigabit Ethernet 1 on unit 1, the prompt displays the object type and unit (for example, Gi1/0/1).

[# | >] — The # sign is used to indicate that the system is in the Privileged Exec mode. The > symbol indicates that the system is in the User Exec mode, which is a read-only mode in which the system does not allow configuration.

**Navigating CLI Command Modes**

Table 2-5 describes how to navigate through the CLI Command Mode hierarchy.

**Table 2-5. Navigating CLI Command Modes**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Exec</td>
<td>The user is automatically in User Exec mode unless the user is defined as a privileged user.</td>
<td>console&gt;</td>
<td>logout</td>
</tr>
</tbody>
</table>
### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Exec</td>
<td>Use the <code>enable</code> command to enter into this mode. This mode is password protected.</td>
<td><code>console#</code></td>
<td>Use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to return to the User Exec mode.</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>From Privileged Exec mode, use the <code>configure</code> command.</td>
<td><code>console(config)#</code></td>
<td>Use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to return to the Privileged Exec mode.</td>
</tr>
<tr>
<td>Line Interface</td>
<td>From Global Configuration mode, use the <code>line</code> command.</td>
<td><code>console(config-line)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>BGP Router Configuration</td>
<td>From Global Configuration mode, use the <code>router bgp</code> command.</td>
<td><code>console(config-router)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>Command Mode</td>
<td>Access Method</td>
<td>Command Prompt</td>
<td>Exit or Access Previous Mode</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 Address Family Configuration</td>
<td>From BGP Router Configuration mode, use the address-family ipv6 command.</td>
<td>console (config-router-af)#</td>
<td>To exit to BGP Router Configuration mode, use the exit command, or press &lt;Ctrl&gt;+&lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>Management Access-List</td>
<td>From Global Configuration mode, use the management access-list command.</td>
<td>console(config-macl)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt;+&lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>Policy-Class-Map</td>
<td>From Global Configuration mode, use the policy-map class command.</td>
<td>console(config-policy-map)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt;+&lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>Class-Map</td>
<td>From Global Configuration mode, use the class-map command.</td>
<td>console(config-classmap)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt;+&lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>Command Mode</td>
<td>Access Method</td>
<td>Command Prompt</td>
<td>Exit or Access Previous Mode</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>MAC Access List</td>
<td>From Global Configuration mode, use the <code>mac access-list</code> command.</td>
<td><code>console(config-mac-access-list)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>SSH Public Key-Chain</td>
<td>From Global Configuration mode, use the <code>crypto key pubkey-chain ssh</code> command.</td>
<td><code>console(config-pubkey-chain)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>SSH Public Key String</td>
<td>From the SSH Public Key-Chain mode, use the `user-key &lt;user name &gt; {rsa</td>
<td>dsa}` command.</td>
<td><code>console(config-pubkey-key)#</code></td>
</tr>
<tr>
<td>TACACS</td>
<td>From Global Configuration mode, use the <code>tacacs-server host</code> command.</td>
<td><code>console(config-tacacs)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
</tbody>
</table>
### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server Configuration</td>
<td>From Global Configuration mode, use the radius server host command.</td>
<td><code>console(Config-auth-radius)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>RADIUS Dynamic Authorization</td>
<td>From Global Configuration, use the aaa server radius dynamic-author command.</td>
<td><code>console(config-radius-da)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>SNMP Host Configuration</td>
<td>From Global Configuration mode, use the snmp-server command.</td>
<td><code>console(config-snmp)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>SNMP v3 Host Configuration</td>
<td>From Global Configuration mode, use the snmp-server v3-host command.</td>
<td><code>console(config-snmp)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
</tbody>
</table>
### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Community Configuration</strong></td>
<td>From Global Configuration mode, use the <code>snmp-server community</code> command.</td>
<td><code>console(config-snmp)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
<tr>
<td><strong>Crypto Certificate Generation</strong></td>
<td>From Global Configuration mode, use the <code>crypto certificate number generate</code> command.</td>
<td><code>console(config-crypto-cert)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
<tr>
<td><strong>Crypto Certificate Request</strong></td>
<td>From Privileged Exec mode, use the <code>crypto certificate number request</code> command.</td>
<td><code>console(config-crypto-cert)#</code></td>
<td>To exit to Privileged Exec mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code></td>
</tr>
<tr>
<td><strong>Stack</strong></td>
<td>From Global Configuration mode, use the <code>stack</code> command.</td>
<td><code>console(config-stack)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
</tbody>
</table>
### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>From Global Configuration mode, use the logging command.</td>
<td>console(config-logging)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt; + &lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>MST</td>
<td>From Global Configuration mode, use the spanning-tree mst configuration command.</td>
<td>console(config-mst)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt; + &lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>VLAN Config</td>
<td>From Global Configuration mode, use the vlan command.</td>
<td>console(config-vlan)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt; + &lt;Z&gt; to Privileged Exec mode.</td>
</tr>
<tr>
<td>Router OSPF</td>
<td>From Global Configuration mode, use the router ospf command.</td>
<td>console(config-router)#</td>
<td>To exit to Global Configuration mode, use the exit command, or press &lt;Ctrl&gt; + &lt;Z&gt; to Privileged Exec mode.</td>
</tr>
</tbody>
</table>
### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Router Config</td>
<td>From Global Configuration mode, use the <code>ip vrf</code> command.</td>
<td><code>console(config-vrf-XXX)#</code> where XXX is the VRF name.</td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
<tr>
<td>Router RIP Config</td>
<td>From Global Configuration mode, use the <code>router rip</code> command.</td>
<td><code>console(config-router)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
<tr>
<td>Router OSPFv3 Config</td>
<td>From Global Configuration mode, use the <code>ipv6 router ospf</code> command.</td>
<td><code>console(config-rtr)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
<tr>
<td>IPv6 DHCP Pool Mode</td>
<td>From Global Configuration mode, use the <code>ipv6 dhcp pool</code> command.</td>
<td><code>console(config-dhcp6s-pool)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt;+&lt;Z&gt;</code> to Privileged Exec mode</td>
</tr>
</tbody>
</table>

### Interface Configuration Modes
Using the CLI

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>From Global Configuration mode, use the <code>interface gigabitethernet</code> command. Or, use the abbreviation <code>interface gi</code>.</td>
<td><code>console (config-if-Giunit/slot/port)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>Ctrl</code> + <code>&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>10 Gigabit Ethernet</td>
<td>From Global Configuration mode, use the <code>interface tengigabitethernet</code> command. Or, use the abbreviation <code>interface te</code>.</td>
<td><code>console (config-if-Teunit/slot/port)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>Ctrl</code> + <code>&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>40 Gigabit Ethernet</td>
<td>From Global Configuration mode, use the <code>interface fortygigabitethernet</code> command. Or, use the abbreviation <code>interface fo</code>.</td>
<td><code>console (config-if-Founit/slot/port)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>Ctrl</code> + <code>&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>Port Channel</td>
<td>From Global Configuration mode, use the <code>interface port-channel</code> command. Or, use the abbreviation <code>interface po</code>.</td>
<td><code>console (config-if-poport-channel-number)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>Ctrl</code> + <code>&lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
</tbody>
</table>
### Starting the CLI

To begin running the CLI, perform the following steps:

1. Start the switch and wait until the startup procedure is complete and the User Exec mode is entered. The prompt `console>` is displayed.

2. Configure the switch and complete any required tasks.

### Table 2-5. Navigating CLI Command Modes (continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Command Prompt</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>From Global Configuration mode, use the <code>interface vlan vlan-id</code> command.</td>
<td><code>console(config-if-vlanvlan-id)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt; + &lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>From Global Configuration mode, use the <code>interface tunnel tunnel-id</code> command. Or, use the abbreviation <code>interface tu</code>.</td>
<td><code>console(config-tunneltunnel-id)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt; + &lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
<tr>
<td>Loopback</td>
<td>From Global configuration mode, use the <code>interface loopback loopback-id</code> command. Or, use the abbreviation <code>interface lo</code>.</td>
<td><code>console(config-if-loopbackloopback-id)#</code></td>
<td>To exit to Global Configuration mode, use the <code>exit</code> command, or press <code>&lt;Ctrl&gt; + &lt;Z&gt;</code> to Privileged Exec mode.</td>
</tr>
</tbody>
</table>
When finished, exit the session with the `quit` or `exit` command.

The switch can be managed over a direct connection to the switch console port or through a Telnet connection. If access is through a Telnet connection, the switch must have a defined IP address, corresponding management access granted, and a connection to the network.

### Using CLI Functions and Tools

The CLI has been designed to manage the switch’s configuration file system and to manage switch security. A number of resident tools exist to support these and other functions.

#### Configuration Management

All managed systems have software images and databases that must be configured, backed up and restored. Two software images may be stored on the system, but only one of them is active. The other one is a backup image. The same is true for configuration files, which store the configuration parameters for the switch. The system has three configuration files. One file is a memory-only file and is the current configuration file for the switch. The second file is the one that is loaded by the system when it reboots. There is one backup configuration file. The system also provides methods to back up these files to a remote system.

#### File System Commands

All files are stored in a file system. The commands shown in Table 2-6 are used to perform operations on these files.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete file</td>
<td>Deletes file.</td>
</tr>
<tr>
<td>filedescr file description</td>
<td>Adds a description to a file (up to 128 characters can be used).</td>
</tr>
<tr>
<td>copy source destination</td>
<td>Copies a file from source file to destination file.</td>
</tr>
</tbody>
</table>
Copying Files

The `copy` command not only provides a method for copying files within the file system, but also to and from remote servers. With the `copy` command and URLs to identify files, the user can back up images to local or remote systems or restore images from local or remote systems.

To use the `copy` command, the user specifies the source file and the destination file. For example, `copy tftp://remotehost/pub/backupfile backup-config` copies a file from the remote TFTP server to a local backup configuration file. In this case, if the local configuration file does not exist, then it is created by the command. If it does exist, it is overwritten. If there is not enough space on the local file system to accommodate the file, an error is flagged.

Refer to the `copy` command description in the Layer 2 commands section of the guide for command details.

Referencing External/Internal File systems

Configuration or software images are copied to or retrieved from remote systems using the TFTP or FTP protocols.

- `tftp://server-name/path/filename` — identifies a file on a remote TFTP server identified by the server-name. Trivial file transfer protocol is a simplified FTP and uses a UDP port instead of TCP and does not have password protection.

- `<ftp://{user@ipaddress | hostname}/filepath/filename>` — Identifies a file on a remote FTP server identified by the server-name. The File Transfer Protocol (FTP) is a standardized protocol used to transfer files over the network using TCP. FTP is optionally secured with a clear-text user name and password.

Special System Files

The following special filenames are used to refer to special virtual system files, which are under control of the system and may not be removed or added. These file names are reserved and may not be used as user-defined files. When the user copies a local source file into one of these special files and the source file has an attached file description, it also is copied as the file description for the special file.

- `backup-config` — This file refers to the backup configuration file.
• **running-config** — This file refers to the configuration file currently active in the system. It is possible to copy the running-config image to a backup-config file or to the startup-config file.

• **startup-config** — This file refers to the special configuration image stored in flash memory which is loaded when the system next reboots. The user may copy a particular configuration file (remote or local) to this special file name and reboot the system to force it to use a particular configuration.

• **active & backup** — These files refer to software images. The active image will be loaded when the system next reboots. Either the active or backup can be chosen for the next reboot using the command `boot system`.

The CLI prevents the user from accidentally copying a configuration image onto a software image and vice versa.

**Management Interface Security**

This section describes the minimum set of management interface security measures implemented by the CLI. Management interface security consists of user account management, user access control and remote network/host access controls.

**CLI through Telnet, SSH, Serial Interfaces**

The CLI is accessible through a local serial interface/console port, the out-of-band interface, or in-band interfaces. Since the console port requires a physical connection for access, it is used if all else fails. The console port interface is the only interface from which the user may access the Easy Setup Wizard. It is the only interface that the user can access if the remote authentication servers are down and the user has not configured the system to revert to local managed accounts.

The following rules and specifications apply to these interfaces:

• The CLI is accessible from remote telnet through the IP address for the switch. IP addresses are assigned separately for the out-of-band interface and the in-band ports.

• The CLI is accessible from a secure shell interface.

• The administrator generates keys for SSH locally via the CLI.
• The serial session defaults to 9600 BAUD, eight data bits, one stop bit, no parity and no flow control (115200 for the N1100-ON, N2100-ON, and N3100-ON).

User Accounts Management

The CLI provides configuration of authentication for switch administrators or network users either through remote authentication servers supporting TACACS+ or RADIUS or through a set of locally managed user accounts. The setup wizard asks the user to create the initial administrator account and password at the time the system is booted.

The following rules and specifications apply:

• The administrator may create additional administrator accounts.
• User accounts have an associated privilege level, a user name, and a user password.
• The administrator is able to delete the administrator accounts.
• The password is saved internally in encrypted format and never appears in clear text anywhere on the CLI.
• The CLI supports TACACS+ and RADIUS authentication servers and RADIUS accounting servers.
• The CLI allows the administrator to configure primary and secondary authentication servers. If the primary authentication server fails to respond within a configurable period, the CLI automatically tries the secondary authentication server.
• The administrator can specify whether the CLI should revert to using local accounts when the remote authentication servers do not respond or if the CLI simply fails the login attempt because the authentication servers are down. This capability applies only when the administrator is logged in through a telnet or an SSH session.
• The CLI always allows the administrator to log in to a local serial port even if the remote authentication server(s) are down. In this case, CLI reverts to using the locally configured accounts to allow the administrator to log in.
**User Access Control**

In addition to authenticating an administrator, the CLI also assigns the administrator access to one of two security levels. Privilege level 1 has read-only access. This level allows the administrator to read information but not configure the switch. The access to this level cannot be modified. Level 15 is the special access level assigned to the superuser of the switch. This level has full access to all functions within the switch.

If the account is created and maintained locally, each account is given an access level at the time of account creation. If the administrator is authenticated through remote authentication servers, the authentication server is configured to pass the access level to the CLI when the account is authenticated. When RADIUS is used, the Vendor-Specific Option field returns the access level. Two vendor specific options are supported. These are CISCO-AV-Pairs(Shell:priv-lvl=x) and Dell RADIUS VSA (user-group=x). TACACS+ provides the appropriate level of access.

The following rules and specifications apply:

- The administrator determines whether remote authentication servers or locally defined authentication accounts are used.
- If authentication servers are used, the administrator can identify at least two remote servers (the user may choose to configure only one server) and what protocol to use with the server, TACACS+ or RADIUS. One of the servers is primary and the other is the secondary server (the user is not required to specify a secondary server). If the primary server fails to respond in a configurable time period, the CLI automatically attempts to authenticate the user with the secondary server.
- The administrator is able to specify what happens when both primary and secondary servers fail to respond. In this case, the user is able to indicate that the CLI should either use the local user accounts or reject all requests.
- Even if the administrator configures the CLI to fail login when the remote authentication servers are down, the CLI allows access via the serial interface authenticated by locally managed account data. The default for serial port access is no login or password required.
SYSLOG

The switch supports sending logging messages to a remote SYSLOG server. The administrator configures a remote log server to which SYSLOG messages are sent.

The following rules apply:

- The administrator configures a remote SYSLOG server to which system logging messages are sent.
- Log messages are implementation-dependent but may contain debug messages, security or fault events.
- The switch maintains at most the last 1000 system events in the in-memory log.

Security Logs

The system log records security events including the following:

- User login.
- User logout.
- Denied login attempts.
- User attempt to exceed security access level.
- Denied attempts by external management system to access the system.

The security log record contains the following information:

- The login name, if available, or the protocol being accessed if the event is related to a remote management system.
- The IP address from which the user is connecting or the IP address of the remote management system.
- A description of the security event.
- A timestamp of the event

If a SYSLOG server is configured and available, the switch sends security records to the configured servers.
Management ACL

In addition to user access control, the system also supports filtering of management protocol packets addressed to the switch over the in-band ports. This capability allows individual hosts or subnets to access the switch using specific management protocols.

The administrator defines a management profile, which identifies management protocols such as the following:

- Telnet.
- SSH and the keying information to use for SSH.
- HTTP.
- HTTPS and the security certificate to be used.
- SNMPv1/v2c and the read and read/write community strings to be used.
- SNMPv3 and the security information for used this protocol.

For each of these management profiles, the administrator defines the list of hosts or subnets from which the management profiles may be used. The management ACL capability only applies to in-band ports and may not be configured on the out-of-band management port.

Other CLI Tools and Capabilities

The CLI has several other capabilities associated with its primary functions.

Terminal Paging

The default terminal width and length for CLI displays is 79 characters and 25 lines, respectively. The length setting is used to control the number of lines the CLI will display before it pauses. For example, the CLI pauses at 24 lines and prompts the user with the --More-- or (q)uit prompt on the 25th line. The CLI waits for the user to press either <q> or <Enter> or any other key. If the user presses any key other than <Enter> or <q>, the CLI shows the next page. A <q> key stops the display and returns to the CLI prompt. The <Enter> key advances the display by one line. Use the terminal length command to change the number of lines displayed in a page. A terminal length of 0 disables pagination. This option is not recommended for serial console speeds of less than 115200.
**Boot Message**

The boot message is a system message that is not user-configurable and is displayed when the system is booting.

To start the normal booting process, select item 1 in the Boot Menu. The following is a sample log for booting information.

Select startup option within 5 seconds, else Operational Code will start automatically...

Operational Code Startup -- Main Menu

1 - Start Operational Code
2 - Display Boot Menu

Select (1, 2)#
active = /dev/mtd7
Extracting Operational Code from .stk file...done.
Loading Operational Code...done.
Decompressing Operational Code...done.
Scanning devshell symbols file...
47544 symbols, loading...
Done.
PCI unit 0: Dev 0xb842, Rev 0x02, Chip BCM56842_A0, Driver BCM56840_B0
SOC unit 0 attached to PCI device BCM56842_A0
Adding BCM transport pointers
Configuring CFUTRANS TX
Configuring CFUTRANS RX

<186> Aug 26 08:18:23 0.0.0.0-1 General[72162340]: bootos.c(166) 4 %%
Event(0xaaaaaaaa) started!

(Unit 1 - Waiting to select management unit)>
Applying Global configuration, please wait ...

Applying Interface configuration, please wait ...

**Boot Utility Menu**

If a user is connected through the serial interface during the boot sequence, the operator is presented with the option to enter the Boot Utility Menu during the boot sequence. Selecting item 2 displays the menu and may be typed only during the initial boot up sequence.

Select startup option within 5 seconds, else Operational Code will start automatically...

Operational Code Startup -- Main Menu
1 - Start Operational Code
2 - Display Boot Menu

Select (1, 2)# 2

Enter the Boot Menu password: calvin

Boot Menu Rev: 6.0

Operational Code -- Boot Main Menu

1  - Start Operational Code
2  - Select Baud Rate
3  - Retrieve Logs
4  - Load New Operational Code
5  - Display Operational Code Details
9  - Reboot
10 - Restore Configuration to Factory Defaults
11 - Activate Backup Image
12 - Start Password Recovery

Enter Choice# 4

Creating tmpfs filesystem on /mnt/download for download...done.
Current Active Image# /dev/mtd7
Which Image to Update Active (/dev/mtd7) OR Back-Up (/dev/mtd6)? Select (A/B): B
You selected to update Back-Up Image /dev/mtd6...
Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM) []:T

Please ensure TFTP server is running to begin Transfer...
Enter Server IP []: 10.27.9.99
Enter Host IP []: 10.27.22.99
Enter Host Subnet Mask [255.255.255.0]: 255.255.252.0
Enter Gateway IP []: 10.27.20.1
Enter Filename []: jmclendo/N4000v6.0.0.8.stk
Do you want to continue? Press(Y/N): y
Bringing up eth0 interface...done.
Adding default gateway 10.27.20.1 to the Routing Table...done.
Bringing down eth0 interface...done.
Erasing /dev/mtd6!!!
Erasing 128 Kibyte @ 17e0000 -- 99 % complete.
Updating code file...
Code Update Instructions Found!
Critical components modified on Back-Up Partition -- Please activate Back-Up Image to load the same on Reboot

Do you wish to activate Back-Up Image? (Y/N): 
Cleaning tmpfs filesystem on /mnt/download...done.
Enter Choice# 5
active = /dev/mtd7
Extracting Operational Code from .stk file...done.
Loading Operational Code...done.
Decompressing Operational Code...done.
Product Details:

  Operational Code Image File Name - N4000v6.0.0.8
  Rel 6, Ver 0, Maint Lev 0, Bld No 8
  Timestamp - Thu Aug 22 13:09:33 EDT 2013
  Number of components - 1
  Device 776
  ImageFlags 1
  L7_MODULE_LIST=linux-kernel-bde.ko linux-user-bde.ko

Enter Choice# 10

Are sure you want to Erase Current Configuration? (Y/N): y
Erasing Current Configuration...done.

Boot Menu Rev: 6.0

Operational Code -- Boot Main Menu

  1  - Start Operational Code
  2  - Select Baud Rate
  3  - Retrieve Logs
  4  - Load New Operational Code
  5  - Display Operational Code Details
  9  - Reboot
 10  - Restore Configuration to Factory Defaults
 11  - Activate Backup Image
 12  - Start Password Recovery

Enter Choice# 11

Current Active Image# /dev/mtd7
Checking for valid back-up image at /dev/mtd6...done.
Activating Back-Up Image /dev/mtd6...done.
Code Update Instructions Found!
Back-Up Image on /dev/mtd6 Activated -- System Reboot Recommended!

Reboot? (Y/N):
Enter Choice# 12

Starting Operational Code for Password Recovery...
active = /dev/mtd6
Extracting Operational Code from .stk file...done.
Loading Operational Code...done.
Decompressing Operational Code...done.
4 START_OPR_CODE_PASSWD_RECOVERY MODE
Uncompressing apps.lzma
SyncDB Running...
DMA pool size: 16777216
PCI unit 0: Dev 0xb842, Rev 0x02, Chip BCM56842_A1, Driver BCM56840_B0
SOC unit 0 attached to PCI device BCM56842_A1
hpc - No stack ports. Starting in stand-alone mode.

<186> Jul 12 02:40:46 0.0.0.0-1 General[63446620]: bootos.c(179) 11 %
Event(0xaaaaaaaa)                  started!

(Unit 1 - Waiting to select management unit)>

Applying Global configuration, please wait ...

Welcome to Dell Easy Setup Wizard

The setup wizard guides you through the initial switch configuration, and
gets you up and running as quickly as possible. You can skip the setup
wizard, and enter CLI mode to manually configure the switch. You must
respond to the next question to run the setup wizard within 60 seconds,
otherwise the system will continue with normal operation using the default
system configuration. Note: You can exit the setup wizard at any point
by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question within
60 seconds)? [Y/N] n

Thank you for using the Dell Easy Setup Wizard. You will now enter CLI mode.

Applying Interface configuration, please wait ...

**Booting without a Startup Configuration**

When the system boots without a startup configuration (which is not the
same as an empty startup-config) and no EULA Accept file exists on the stack
master, the following prompt occurs:

(Unit 1 - Waiting to select management unit)>
Applying Global configuration, please wait...

SupportAssist EULA
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. 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 the set 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.

AeroHive HiveManager NG EULA
This switch includes a feature that enables it to work with HiveManager (an optional management suite), by sending the switch’s service tag number to HiveManager to authenticate your entitlement to use HiveManager. If you wish to disable this feature, you should run command “eula-consent hiveagent reject” immediately upon powering up the switch for the first time, or at any time thereafter.

Welcome to Dell Easy Setup Wizard

The setup wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question within 60 seconds)? (y/n)

Regardless of if the administrator runs or does not run the Easy Setup wizard and if the SupportAssist application is installed:

```
eula-consent support-assist accept
```

is entered into the running-config if the SupportAssist EULA Accept file exists on the stack master and contains the ‘EULA: Accepted’ text.

Regardless of whether the administrator runs or does not run the Easy Setup wizard and if the HiveAgent is installed:

```
eula-consent hiveagent accept
```
is entered into the running-config if the HiveAgent EULA Accept file exists on the stack master and contains the ‘EULA: Accepted’ text.

The Easy Setup Wizard also prompts the user to configure a proxy server as follows:

Step 5:
Would you like to configure the address of an HTTPS proxy server used by the SupportAssist agent? [Y/N] y
Enter the IPv4 or IPv6 address of the proxy server: 192.168.0.3
Enter the port number used by HTTPS [443]:
Enter the user name required to access the proxy server:
Enter the password required to access the proxy server:

This is the configuration information that has been collected:

User Account setup = admin
Password = ********
Out-of-band IP address = DHCP
VLAN1 Router Interface IP = 0.0.0.0 0.0.0.0
Proxy Server Address: 192.168.0.3
Proxy Server Port: 443
Proxy Server User Name: 
Proxy Server Password: 

**Monitoring Traps from CLI**

It is possible to connect to the CLI session and monitor the events or faults that are being sent as traps from the system. This feature is equivalent to the alarm-monitoring window in a typical network management system. The user enables display of events or monitor traps from the CLI by entering the command `logging console`. Traps generated by the system are dumped to all CLI sessions that have requested monitoring mode to be enabled. The `no logging console` command disables trap monitoring for the session. By default, console logging is enabled. Use the terminal monitor command to observe logging messages when connected via telnet or SSH.

**Viewing System Messages**

System messages autonomously display information regarding occurrences that may affect switch operations. By default, system messages are not displayed on CLI sessions connected via telnet or SSH. Use the `terminal monitor` command to enable the autonomous display of system messages when connecting to the switch via telnet or SSH. System messages are always displayed on the serial console.
Layer 2 Switching Commands

The sections that follow describe commands that conform to the OSI model data link layer (Layer 2). Layer 2 commands provide a logical organization for transmitting data bits on a particular medium. This layer defines the framing, addressing, and checksum functions for Ethernet packets.

This section of the document contains the following Layer 2 topics:

<table>
<thead>
<tr>
<th>ACL Commands</th>
<th>Ethernet Configuration Commands</th>
<th>IPv6 Access List Commands</th>
<th>MLAG Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address Table</td>
<td>Ethernet CFM Commands</td>
<td>IPv6 Access List Commands</td>
<td>Port Channel Commands</td>
</tr>
<tr>
<td>Commands</td>
<td>Green Ethernet Commands</td>
<td>IPv6 MLD Snooping</td>
<td>Port Monitor Commands</td>
</tr>
<tr>
<td>Auto-VoIP Commands</td>
<td></td>
<td>Commands</td>
<td>QoS Commands</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDP</td>
<td>GMRP Commands</td>
<td>IPv6 MLD Snooping</td>
<td></td>
</tr>
<tr>
<td>Interoperability</td>
<td></td>
<td>Querier Commands</td>
<td>IP Source Guard Commands</td>
</tr>
<tr>
<td>Commands</td>
<td></td>
<td></td>
<td>Spanning Tree Commands</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDLD Commands</td>
</tr>
<tr>
<td>DHCP Layer 2 Relay</td>
<td>IGMP Snooping Commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>IGMP Snooping Querier Commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCPv6 Snooping</td>
<td>Interface Error Disable and Auto</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td>Recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic ARP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inspection Commands</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Layer 2 Switching Commands | 265
ACL Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Access to a switch or router can be made more secure through the use of Access Control Lists (ACLs) to control the type of traffic allowed into or out of specific ports. An ACL consists of a series of rules, each of which describes the type of traffic to be processed and the actions to take for packets that meet the classification criteria. Rules within an ACL are evaluated sequentially until a match is found, if any. An implicit deny-all rule is added after the end of the last configured access group. ACLs can help ensure that only authorized users have access to specific resources while blocking out any unwarranted attempts to reach network resources.

ACLs may be used to restrict contents of routing updates, decide which types of traffic are forwarded or blocked and, above all, provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network.

The Dell EMC Networking ACL feature allows classification of packets based upon Layer 2 through Layer 4 header information. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique EtherType value; thus, all IPv4 and IPv6 classifiers implicitly include the EtherType field.

Multiple ACLs per interface are supported. The ACLs can be a combination of Layer 2 and/or Layer 3/4 ACLs. ACL assignment is appropriate for both Ethernet ports and LAGs. ACLs can also be time based. The maximum number of ACLs and rules supported depends on the resources consumed by other processes and configured features running on the switch.

ACL Logging

Access list rules are monitored in hardware to either permit or deny traffic matching a particular classification pattern, but the network administrator currently has no insight as to which rules are being matched. Dell EMC Networking platforms have the ability to count the number of matches for a
particular classifier rule. The ACL logging feature allows these hardware "hit" counts to be collected on a per-rule basis and reported periodically to the network administrator using the system logging facility and an SNMP trap.

The Dell EMC Networking ACL syntax supports a log parameter that enables hardware hit count collection and reporting. A five minute logging interval is used, at which time trap log entries are written for each ACL logging rule that accumulated a nonzero hit count during that interval. The logging interval is not user configurable.

**How to Build ACLs**

This section describes how to build ACLs that are less likely to exhibit false matches.

Administrators are cautioned to specify ACL access-list, permit and deny rule criteria as fully as is possible in order to avoid false matches. As an example, rules that specify a TCP or UDP port value should also specify the TCP or UDP protocol and the IPv4 or IPv6 Ether type. Rules that specify an IP protocol should also specify the Ether type value for the frame. In general, any rule that specifies matching on an upper layer protocol field should also include matching constraints for each of the lower layer protocols. For example, a rule to match packets directed to the well-known UDP port number 22 (SSH) should also include matching constraints on the IP protocol field (protocol = 0x11 or UDP) and the Ether type field (Ether type = 0x0800 or IPv4). In Table 3-1 is a list of commonly used Ether types and, in Table 3-2 commonly used IP protocol numbers.
### Table 3-1. Common Ethertypes

<table>
<thead>
<tr>
<th>EtherType</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0800</td>
<td>Internet Protocol version 4 (IPv4)</td>
</tr>
<tr>
<td>0x0806</td>
<td>Address Resolution Protocol (ARP)</td>
</tr>
<tr>
<td>0x0842</td>
<td>Wake-on LAN Packet</td>
</tr>
<tr>
<td>0x8035</td>
<td>Reverse Address Resolution Protocol (RARP)</td>
</tr>
<tr>
<td>0x8100</td>
<td>VLAN tagged frame (IEEE 802.1Q)</td>
</tr>
<tr>
<td>0x86DD</td>
<td>Internet Protocol version 6 (IPv6)</td>
</tr>
<tr>
<td>0x8808</td>
<td>MAC Control</td>
</tr>
<tr>
<td>0x8809</td>
<td>Slow Protocols (IEEE 802.3)</td>
</tr>
<tr>
<td>0x8870</td>
<td>Jumbo frames</td>
</tr>
<tr>
<td>0x888E</td>
<td>EAP over LAN (EAPOL – 802.1x)</td>
</tr>
<tr>
<td>0x88CC</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>0x8906</td>
<td>Fibre Channel over Ethernet</td>
</tr>
<tr>
<td>0x8914</td>
<td>FCoE Initialization Protocol</td>
</tr>
<tr>
<td>0x9100</td>
<td>Q in Q</td>
</tr>
</tbody>
</table>

### Table 3-2. Common IP Protocol Numbers

<table>
<thead>
<tr>
<th>IP Protocol Numbers</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>IPv6 Hop-by-hop option</td>
</tr>
<tr>
<td>0x01</td>
<td>ICMP</td>
</tr>
<tr>
<td>0x02</td>
<td>IGMP</td>
</tr>
<tr>
<td>0x06</td>
<td>TCP</td>
</tr>
<tr>
<td>0x08</td>
<td>EGP</td>
</tr>
<tr>
<td>0x09</td>
<td>IGP</td>
</tr>
<tr>
<td>0x11</td>
<td>UDP</td>
</tr>
</tbody>
</table>
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list</code></td>
<td></td>
</tr>
<tr>
<td>`deny</td>
<td>permit` (IP ACL)</td>
</tr>
<tr>
<td>`deny</td>
<td>permit` (Mac-Access-List-Configuration)</td>
</tr>
<tr>
<td><code>ip access-group</code></td>
<td></td>
</tr>
<tr>
<td><code>mac access-group</code></td>
<td></td>
</tr>
<tr>
<td><code>mac access-list extended</code></td>
<td></td>
</tr>
<tr>
<td><code>no ip access-list list-name</code></td>
<td></td>
</tr>
</tbody>
</table>

**ip access-list**

Use the `ip access-list` command in Global Configuration mode to create an Access Control List (ACL) that is identified by the parameter `list-name` and to enter IPv4-Access-List configuration mode. If parameterized with the name of an existing access list, additional match clauses are added to the end of the access list.

```
ip access-list list-name [extended]
```

```
no ip access-list list-name
```

- list-name—Access-list name up to 31 characters in length.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

Access lists use the extended access list format. Multiple permit and deny clauses and actions may be specified without requiring the access list name to be entered each time. Permit and deny clauses are entered in order from the first match clause when in Access List Configuration mode.
ACL names are global. An IPv6 access list cannot have the same name as an IPv4 access list. Access list names can consist of any printable character except a question mark. Names can be up to 31 characters in length. ACLs referenced in a route map may not be edited. Instead, create a new ACL with the desired changes and refer to the new ACL in the route map.

**deny | permit (IP ACL)**

Use this command in Ipv4-Access-List Configuration mode to create a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list if no sequence number is specified. Use the no form of the command to delete an existing permit/deny clause.

**Syntax**

```
[sequence-number] {deny | permit} {ipv4-protocol | 0-255 | every} {srcip srcmask | any | host srcip} [{range {portkey | startport} {portkey | endpoint}} | {eq | neq | lt | gt} {portkey | 0-65535} | {dstip dstmask | any | host dstip} [{range {portkey | startport} {portkey | endpoint}} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} interface-id] [rate-limit rate burst-size]
```

**no <sequence-number>**

- [sequence-number]—Identifies the order of application of the permit/deny statement. If no sequence number is assigned, permit/deny statements are assigned a sequence number beginning at 1000 and incrementing by 10. Statements are applied in hardware beginning with the lowest sequence number. Sequence numbers only have applicability within an access group, i.e. the ordering applies within the access-group scope. The range for sequence numbers is 1–2147483647.
- {deny | permit}—Specifies whether the IP ACL rule permits or denies the matching traffic.
- {ipv4-protocol | number | every}—Specifies the protocol to match for the IP ACL rule.
IPv4 protocols: eigrp, gre, icmp, igmp, ip, ipinip, ospf, tcp, udp, pim, arp, sctp

- number: a protocol number in decimal, for example, 8 for EGP
- every: Match any protocol (don’t care)

srcip srcmask | any | host srcip—Specifies a source IP address and netmask to match for the IP ACL rule.

- Specifying “any” implies specifying srcip as “0.0.0.0” and srcmask as “255.255.255.255” for IPv4.
- Specifying “host A.B.C.D” implies srcip as “A.B.C.D” and srcmask as “0.0.0.0”.

- [{eq | neq | lt | gt} {portkey | number} | range startport endport} | Specifies the layer 4 source or destination port match condition for the TCP/UDP ACL rule. When the protocol is SCTP, TCP or UDP, a source or destination port number, which ranges from 0-65535, or a portkey, which can be one of the following keywords: domain, echo, ftp, ftp-data, http, smtp, snmp, telnet, tftp, www, bgp, pop2, pop3, ntp, rip, time, who may be entered. Each of these keywords translates into its equivalent destination port number.

- When “range” is specified, IP ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range.

- When “eq” is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey.

- When “lt” is specified, IP ACL rule matches if the layer 4 destination port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>.

- When “gt” is specified, IP ACL rule matches if the layer 4 destination port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535.
When “neq” is specified, IP ACL rule matches only if the layer 4 destination port number is not equal to the specified port number or portkey.

IPv4 TCP/UDP port names: domain, echo, ftp, ftp-data, http, smtp, snmp, telnet, tftp, www, bgp, pop2, pop3, ntp, rip, time, who

- dstip dstmask | any | host dstip—Specifies a destination IP address and netmask for match condition of the IP ACL rule.
- Specifying “any” implies specifying dstip as “0.0.0.0” and dstmask as “255.255.255.255”.
- Specifying “host A.B.C.D” implies dstip as “A.B.C.D” and dstmask as “0.0.0.0”.

- [precedence precedence | tos tos [tosmask] | dscp dscp]—Specifies the TOS for an IP/TCP/UDP ACL rule depending on a match of precedence or DSCP values using the parameters dscp, precedence, or tos tosmask.

- flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]—Specifies that the IP/TCP/UDP ACL rule matches on the TCP flags.
  - Ack – Acknowledgment bit
  - Fin – Finished bit
  - Psh – push bit
  - Rst – reset bit
  - Syn – Synchronize bit
  - Urg – Urgent bit
  - When “+<tcpflagname>” is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header.
  - When “-<tcpflagname>” is specified, a match occurs if specified <tcpflagname> flag is *NOT* set in the TCP header.
  - When “established” is specified, a match occurs if either the RST or ACK bits are set in the TCP header.
  - This option is visible only if protocol is “tcp”.

- When icmp-type is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255.
- When icmp-code is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255.
- Specifying icmp-message implies both icmp-type and icmp-code are specified.
- ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type. This option is visible only if the protocol is “icmp”.

• **igmp-type** — When igmp-type is specified, IP ACL rule matches on the specified IGMP message type (i.e., a number from 0 to 255).

• **fragments** — Specifies the rule matches packets that are non-initial fragments (fragment bit asserted). Not valid for rules that match L4 information such as TCP port number since that information is carried in the initial packet.

• **log** — Specifies that this rule is to be logged if the permit/deny rule has been matched one or more times since the expiry of the last logging interval. The logging interval is 5 minutes.

• **time-range** — time-range-name — Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. (See **Time Ranges Commands** for more information.) If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
• **assign-queue** queue-id—Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned. The queue ID is the internal queue number (traffic class), not the CoS value. Use the `show classofservice` command to display the assignment of CoS and DSCP values to internal queue numbers.

• `{mirror | redirect}` interface-id—Specifies the mirror or redirect Ethernet interface to which packets matching this rule are copied or forwarded, respectively.

• **rate-limit** rate burst-size—Specifies the allowed rate of traffic as per the configured rate in Kbps, and burst-size in kbytes. Rate limits only apply to permit rules.
  - Rate – the committed rate in kilobits per second
  - Burst-size – the committed burst size in Kilobytes.

**Default Configuration**

No ACLs are configured by default. An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.

**Command Mode**

Ipv4-Access-List Configuration mode

**User Guidelines**

Administrators are cautioned to specify permit and deny rule matches as fully as is possible in order to avoid false matches. Rules that specify an IP port value should also specify the protocol (TCP or UDP) and relevant IP addresses or subnets. In general, any rule that specifies matching on an upper layer protocol field should also include matching constraints for lower layer protocol fields. For example, a rule to match packets directed to the well-known UDP port number 22 (SSH) should also include constraints on the IP protocol field (UDP). IPv4 and IPv6 ACLs implicitly include the EtherType in the match criteria. Below is a list of commonly used EtherTypes:

<table>
<thead>
<tr>
<th>Ethertype</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0800</td>
<td>Internet Protocol version 4 (IPv4)</td>
</tr>
</tbody>
</table>
In order to provide the greatest amount of flexibility in configuring ACLs, the permit/deny syntax allows combinations of matching criteria that may not make sense when applied in practice.

Port ranges are not supported for ACLs configured in egress (out) access-groups. This means that only the `eq` operator is supported in an egress (out) ACL.

The protocol type must be `sctp`, `tcp` or `udp` to specify a port range.

The fragment keyword is not supported for ACLs configured in egress (out) IPv4 access-groups.

The rate-limit command is not supported for ACLs configured in egress (out) IPv4 access-groups on the N4000 switches. Rate limits are only valid for permit rules.

Any – is equivalent to `0.0.0.0 255.255.255.255` for IPv4 access lists

Host – indicates specified address with mask equal to `255.255.255.255` and address `0.0.0.0` for IPv4.

<table>
<thead>
<tr>
<th>Ethertype</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0806</td>
<td>Address Resolution Protocol (ARP)</td>
</tr>
<tr>
<td>0x0842</td>
<td>Wake-on LAN Packet</td>
</tr>
<tr>
<td>0x8035</td>
<td>Reverse Address Resolution Protocol (RARP)</td>
</tr>
<tr>
<td>0x8100</td>
<td>VLAN tagged frame (IEEE 802.1Q)</td>
</tr>
<tr>
<td>0x86DD</td>
<td>Internet Protocol version 6 (IPv6)</td>
</tr>
<tr>
<td>0x8808</td>
<td>MAC Control</td>
</tr>
<tr>
<td>0x8809</td>
<td>Slow Protocols (IEEE 802.3)</td>
</tr>
<tr>
<td>0x8870</td>
<td>Jumbo frames</td>
</tr>
<tr>
<td>0x888E</td>
<td>EAP over LAN (EAPOL – IEEE 802.1x)</td>
</tr>
<tr>
<td>0x88CC</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>0x8906</td>
<td>Fibre Channel over Ethernet</td>
</tr>
<tr>
<td>0x8914</td>
<td>FCoE Initialization Protocol</td>
</tr>
<tr>
<td>0x9100</td>
<td>Q in Q</td>
</tr>
</tbody>
</table>
The command accepts the optional `time-range` parameter. The `time-range` parameter allows imposing a time limitation on the IP ACL rule as defined by the parameter `time-range-name`. If a time range with the specified name does not exist, and the IP ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with the specified name exists, and the IP ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with a specified name becomes active. The ACL rule is removed when the time-range with a specified name becomes inactive.

An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.

Every permit/deny rule that does not have a rate-limit parameter is assigned a counter. If counter resources become exhausted, a warning is issued and the rule is applied to the hardware without the counter.

If a permit/deny clause is entered with the same sequence number as an existing rule, an error is displayed and the existing rule is not updated with the new information.

**Command History**

Updated in 6.3.0.1 firmware. Description updated in the 6.4 release.

**Example**

```plaintext
console(config)#ip access-list ipv4
console(config-ip-acl)#100 deny ip any any precedence 3
```

`deny` | `permit` *(Mac-Access-List-Configuration)*

Use the `deny` command in Mac-Access-List Configuration mode to deny traffic if the conditions defined in the deny statement are matched. Use the `permit` command in Mac-Access-List Configuration mode to allow traffic if the conditions defined in the permit statement are matched.

Use this command in Mac-Access-List Configuration mode to create a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list, if no sequence number is specified.

The command is enhanced to accept the optional `time-range` parameter. The `time-range` parameter allows imposing a time limitation on the MAC ACL rule as defined by the parameter `time-range-name`. If a time range with the
specified name does not exist, and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with the specified name exists, and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with a specified name becomes active. The ACL rule is removed when the time-range with a specified name becomes inactive.

Use the `no` form of the command to delete an existing permit/deny clause.

**Syntax**

```
[sequence-number] deny | permit (MAC access-list configuration)
[sequence-number] {deny | permit} {{any | srcmac srcmacmask} {any | bpdu | dstmac dstmacmask}} {ethertypekey | [0x0600-0xFFFF] [vlan {eq 0-4095}] [secondary-vlan {eq 0-4095}] [cos 0-7] [log] [time-range time-range-name] [assign-queue queue-id] [{mirror | redirect} interface-id] [rate-limit rate burst-size]
```

- `sequence-number`—Identifies the order of application of the permit/deny statement. If no sequence number is assigned, permit/deny statements are assigned a sequence number beginning at 1000 and incrementing by 10. Statements are applied in hardware beginning with the lowest sequence number. Sequence numbers only have applicability within an access group, i.e. the ordering applies within the access-group scope. The range for sequence numbers is 1–2147483647.
- `srcmac`—Valid source MAC address in format xxxx.xxxx.xxxx.
- `srcmacmask`—Valid MAC address bit mask for the source MAC address.
- `any`—Packets sent to or received from any MAC address.
- `dstmac`—Valid destination MAC address.
- `destmacmask`—Valid MAC address bit mask for the destination MAC address.
- `bpdu`—Bridge protocol data unit
- `ethertypekey`—Either a keyword or valid four-digit hexadecimal number. (Range: Supported values are appletalk, arp, ibmsna, ipv4, ipv6, ipx, mpls mcast, mpls uc, Netbios, novell, pppoe, rarp.)
- 0x0600-0xFFFF—Specify custom EtherType value (hexadecimal range 0x0600-0xFFFF).

- **vlan eq**—VLAN identifier. (Range 0-4095). This matches the outer VLAN of a single or double-tagged packet. It does not match untagged packets.

- **secondary-vlan eq**—VLAN identifier. (Range 0-4095). This matches the inner VLAN of a double-tagged packet. It does not match single or untagged packets.

- **cos**—Class of service. (Range 0-7)

- **log**—Specifies that this rule is to be logged if the permit/deny rule has been matched one or more times since the expiry of the last logging interval. The logging interval is 5 minutes.

- **time-range-name**—Use the **time-range** parameter to impose a time limitation on the MAC ACL rule as defined by the parameter.

- **assign-queue**—Specifies particular hardware queue for handling traffic that matches the rule.

- **queue-id** —0-6, where n is number of user configurable queues available for that hardware platform. The queue ID is the internal queue number (traffic class), not the CoS value. Use the **show classofservice** command to display the assignment of CoS and DSCP values to internal queue numbers.

- **mirror**—Copies the traffic matching this rule to the specified interface.

- **redirect**—Forwards traffic matching this rule to the specified Ethernet interface.

- **interface-id**—An Ethernet interface identifier, for example gi1/0/12.

- **rate-limit** **rate** **burst-size**—Specifies the allowed rate of traffic per the configured rate in Kbps and burst-size in kbytes. Rate limits only apply to permit rules.
  - **Rate**—The committed rate in kilobits per second
  - **Burst-size**—The committed burst size in Kilobytes.

**Default Configuration**

An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.
**Command Mode**

Mac-Access-List Configuration mode

**User Guidelines**

The assign-queue and redirect parameters are only valid for permit commands.

An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.

Every permit/deny rule that does not have a rate-limit parameter is assigned a counter. If counter resources become exhausted, a warning is issued and the rule is applied to the hardware without the counter.

If a permit|deny clause is entered with the same sequence number as an existing rule, an error is displayed and the existing rule is not updated with the new information.

**Command History**

Updated in 6.3.0.1 firmware. Secondary VLAN option added in 6.3.5 release.

**Example**

The following example configures a MAC ACL to deny traffic from MAC address 0806.c200.0000.

```
console(config)#mac access-list extended DELL123
console(config-mac-access-list)#500 deny 0806.c200.0000 0000.0000.0000 any
```

Use the `ip access-group` command in Global and Interface Configuration modes to apply an IP-based ACL on an interface or a group of interfaces.

Use the `no ip access-group` command to disable an IP-based ACL on an interface or a group of interfaces.

**Syntax**

```
ip access-group name [in | out | control-plane] [seqnum]
no ip access-group name [in | out | control-plane]
```
• name — Access list name. (Range: Valid IP access-list name up to 31 characters in length)
• in — The access list is applied to ingress packets.
• out — The access list is applied to egress packets.
• control-plane — The access list is applied to egress control plane packets only. This is only available in Global Configuration mode.
• seqnum — Precedence for this interface and direction. A lower sequence number has higher precedence. Range: 1 – 4294967295. Default is 1.

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration and Interface Configuration (Ethernet, VLAN, or Port Channel) modes

User Guidelines
The Global Configuration mode command configures the ACL on all Ethernet and port-channel interfaces, whereas the interface mode command does so for the selected interface.

Dell EMC Networking switches support configuration of multiple access groups. Packets are matched against group entries, from lowest sequence number to highest. Configuring an access-group, using the same sequence number as an existing entry, replaces the original group entry.

If the access-list specified in the command does not exist, an error is given.

The ACLs in the access-group are configured in hardware when the interface becomes active. Resource contention issues will only become apparent at that time. It is recommended that ACLs be configured on an active interface as a check prior to deployment in the network.

The optional control-plane keyword allows application of an ACL on the CPU port. Control-plane match actions occur in the egress direction. System level rules are applied on ingress, after application of any user defined ingress rules, therefore, it is not possible to rate limit packets matching the system defined rules with an ACL having a control-plane target. Use the rate-limit cpu command to reduce the effects of low priority traffic on the switch CPU.
An implicit deny-all rule is added after the end of the last access group in each direction (in or out).

**Examples**

```
console(config)#ip access-list aclname
console(config-ip-acl)#exit
console(config)#ip access-group aclname in
console(config)#no ip access-group aclname in
console(config)#ip access-list aclnamel
console(config-ip-acl)#exit
console(config)#ip access-group aclnamel out
console(config)#interface te1/0/1
console(config-if-Tel/0/1)#ip access-group aclname out 2
console(config-if-Tel/0/1)#no ip access-group aclname out
```

**Command History**

Example and description updated in the 6.4 release.

**mac access-group**

Use the `mac access-group` command in Global Configuration or Interface Configuration mode to attach a specific MAC Access Control List (ACL) to an interface.

**Syntax**

```
mac access-group name [in | out | control-plane] [sequence]
no mac access-group name [in | out | control-plane]
```

- **name** — Name of the existing MAC access list. (Range: 1-31 characters)
- **[in | out | control-plane]**— The packet direction. in applies the access-list to ingress packets. out applies the access-list to egress packets. control-plane applies the access-list to ingress control plane packets. control-plane is only valid in Global Configuration mode.
- **sequence** — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1-4294967295)

**Default Configuration**

No ACLs are configured by default.
**Command Mode**

Global Configuration mode or Interface Configuration (Ethernet, VLAN or Port Channel) mode

**User Guidelines**

If the access-list specified in the command does not exist, an error is given. The ACLs in the access-group are configured in hardware when the interface becomes active. Resource contention issues will only become apparent at that time. It is recommended that ACLs be configured on an active interface as a check prior to deployment in the network.

An optional sequence number may be specified to indicate the order of this access-list relative to the other access-lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number already is in use for this interface and direction, the specified access-list replaces the currently attached access list using that sequence number. If the sequence number is not specified for this command, a sequence number is selected that is one greater than the highest sequence number currently in use for this interface and direction.

The optional **control-plane** keyword allows the application of an egress MAC ACL on the CPU port.

This command specified in Interface Configuration mode only affects a single interface.

**Example**

This example rate limits IPv4 multicast traffic ingressing the front panel ports to 8 Kbps and a maximum burst of 4 kilobytes.

```
console(config)# mac access-list extended ipv4-multicast
console(config-mac-access-list)#permit 01:00:5e:00:00:00 00:00:00:ff:ff:ff any rate-limit 8 4
console(config-mac-access-list)#permit any any
```

```
console(config-mac-access-list)#exit
console(config)#mac access-group ipv4-multicast in
```
**mac access-list extended**

Use the **mac access-list extended command** in Global Configuration mode to create the MAC Access Control List (ACL) identified by the name parameter and enter MAC Access-list Configuration mode.

**Syntax**

```
mac access-list extended name
no mac access-list extended name
```

- **name** — Name of the access list. (Range: 1-31 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command to create a mac access control list. The CLI mode is changed to Mac-Access-List Configuration when this command is successfully executed.

**Example**

The following example creates MAC ACL and enters MAC-Access-List-Configuration mode.

```
console(config)#mac access-list extended dell-networking
```

**mac access-list extended rename**

Use the **mac access-list extended rename command** in Global Configuration mode to rename the existing MAC Access Control List (ACL).

**Syntax**

```
mac access-list extended rename name newname
```

- **name** — Existing name of the access list. (Range: 1-31 characters)
• newname — New name of the access list. (Range: 1-31 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
Command fails if the new name is the same as the old one.

**Example**
The following example shows the `mac access-list extended rename` command.

```
console(config)#mac access-list extended DELL1
console(config-mac-access-list)#exit
console(config)#mac access-list extended rename DELL1 DELL2
```

remark

Use the `remark` command to add a comment to an ACL rule. Use the `no` form of the command to remove a comment from an ACL rule.

**Syntax**

```
remark comment
no remark comment
```

• comment—Each remark line is limited to 100 characters. The remark may consist of characters in the range A-Z, a-z, 0-9, and special characters like space, hyphen, underscore. The total length of the remark must not exceed 100 characters.

**Default Configuration**
No remarks are present by default.
**Command Mode**
IPv4 Access-list Configuration mode, IPv6 Access-list Configuration mode, MAC Access-list Configuration mode, ARP Access-list Configuration mode. The **no** form of the command is executed in Global Configuration mode.

**User Guidelines**
The administrator can use the remark keyword to add comments to ACL rule entries belonging to an IPv4, IPv6, MAC or ARP ACL. Remarks are associated with the ACL rule that is created immediately after the remarks are created. When the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in **show running-config** and are not displayed in **show ip access-lists**. The **no remark** command removes the first matching remark from an ACL access-list. Repeated execution of this command with the same remark comment removes the remark from the next ACL rule which associated with the comment (if there is any rule configured with the same comment) or an error message is displayed if there are no matching comments.

**Command History**
Updated in 6.3.0.1 firmware

**Example**

```
calendar(config)#arp access-list new
calendar(config-arp-access-list)#remark “test1”
calendar(config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
calendar(config-arp-access-list)#remark “test1”
calendar(config-arp-access-list)#remark “test2”
calendar(config-arp-access-list)#remark “test3”
calendar(config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
calendar(config-arp-access-list)#permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
calendar(config-arp-access-list)#remark “test4”
calendar(config-arp-access-list)#remark “test5”
calendar(config-arp-access-list)#permit ip host 2.1.1.3 mac host 00:03:04:05:06:01
```
service-acl input

Use the service-acl input command in Interface Configuration mode to block Link Local Protocol Filtering (LLPF) protocol(s) on a given port. Use the no form of this command to unblock link-local protocol(s) on a given port.

Syntax

service-acl input {blockcdp | blockvtp | blockdtp | blockudld | blockpagp | blockssstp | blockall}
no service-acl input [blockcdp | blockvtp | blockdtp | blockudld | blockpagp | blockssstp | blockall]

- **blockcdp**—To block CDP PDU’s from being forwarded.
- **blockvtp**—To block VTP PDU’s from being forwarded.
- **blockdtp**—To block DTP PDU’s from being forwarded.
- **blockudld**—To block UDLD PDU’s from being forwarded.
- **blockpagp**—To block PAgP PDU’s from being forwarded.
- **blockssstp**—To block SSTP PDU’s from being forwarded.
- **blockall**—To block all the PDU’s with MAC of 01:00:00:0c:cc:cx (x-don’t care) from being forwarded.

Default Configuration

The default is that none of the listed protocol PDUs are blocked. UDLD is blocked by default. No other protocol is blocked by default.

Command Mode

Interface Configuration (Ethernet, Port-channel)

User Guidelines

To specify multiple protocols, enter the protocol parameters together on the command line, separated by spaces. This command may be entered multiple times and will block all protocols identified in the arguments. This command is not supported on the N1500 Series switches.

Example

```
console(config-if-Tel/0/1)#service-acl input blockall
```
**show service-acl interface**

This command displays the status of LLPF rules configured on a particular port or on all the ports.

**Syntax**

```
show service-acl interface {interface-id | all}
```

- **interface-id**—An Ethernet interface identifier or a port channel interface identifier. See Interface Naming Conventions for interface representation.

**Default Configuration**

UDLD is blocked by default. No other protocol is blocked by default.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command is not supported on the N1500 Series switches.

**Example**

```
console#show service-acl interface te1/0/1

console(config-if-Te1/0/1)#show service-acl interface te1/0/1
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>Disabled</td>
</tr>
<tr>
<td>VTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>DTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>UDLD</td>
<td>Enabled</td>
</tr>
<tr>
<td>PAGP</td>
<td>Disabled</td>
</tr>
<tr>
<td>SSTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>ALL</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
show access-lists interface

Use the show access-lists interface command to display interface ACLs.

Syntax

show access-lists interface {interface-id {in | out}} | control-plane

- interface-id—The interface identifier (Ethernet, port-channel, or VLAN).
- in—Show the ingress ACLs.
- out—Show the egress ACLs.
- control-plane—Show the control plane ACLs.

Default Configuration

No ACLs are configured by default.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

There are no user guidelines for this command.

Examples

crashConsole#show access-lists interface control-plane

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>ACL Name</th>
<th>Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6</td>
<td>ip61</td>
<td>1000</td>
</tr>
</tbody>
</table>

show ip access-lists

Use the show ip access-lists command to display an IP ACL and time-range parameters.

Syntax

show ip access-lists [accesslistname]
• accesslistname—The name used to identify the IP ACL.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command displays information about the attributes “icmp-type”, “icmp-code”, “igmp-type,” “fragments,” “routing,” and “source and destination L4 port ranges.” It displays the committed rate, committed burst size and the ACL rule hit count of packets matching the ACL rule. This matching packet counter value rolls over upon reaching the maximum value (18446744073709551615 or 2^64 -1).

For an ACL with multiple match rules, processing occurs in order until a rule is matched. Only the counter associated with the matching rule is incremented. (e.g., consider an ACL with three rules, rule 1 does not match, and rule 2 is matched. Rule 3 is not processed. The counters for rule 1 and rule 3 are not incremented.)

If an ACL rule is configured with a rate limit, the counter value is the matched packet count (i.e., both the forwarded and dropped packets are counted). If an ACL rule is configured without a rate limit, the counter value is the count of either the permitted or denied packets.

ACL counters do not interact with DiffServ policies. ACL counters do not interact with PBR counters.

ACL hit counters are associated with the ACL, not the interface on which the ACL is applied. An ACL applied to multiple interfaces will display identical (or nearly identical) counts for each interface. The count displayed is the sum of matching packets received or transmitted on all associated interfaces.

Command History
Updated in 6.3.0.1 firmware.
Examples

The following example displays the configured IP ACLs.

```
console(config)#show ip access-lists
```

Current number of ACLs: 4  Maximum number of ACLs: 100

<table>
<thead>
<tr>
<th>ACL Name</th>
<th>Rules</th>
<th>Count</th>
<th>Interface(s)</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>TO_FRM</td>
<td>2</td>
<td>437</td>
<td>Gi1/0/26</td>
<td>Inbound</td>
</tr>
<tr>
<td>UPLINKS</td>
<td>5</td>
<td>0</td>
<td>Gi1/0/26</td>
<td>Outbound</td>
</tr>
<tr>
<td>Allow-192-168-0-x</td>
<td>3</td>
<td>7617636</td>
<td>Gi1/0/29</td>
<td>Inbound</td>
</tr>
</tbody>
</table>

The following example displays the IP ACLs configured on a device.

```
console#show ip access-lists asdasd
```

IP ACL Name: asdasd

Inbound Interface(s):
Gi1/0/7

Rule Number: 1
Action................................. permit
Match All.............................. FALSE
Protocol............................... 6(tcp)
Source IP Address..................... 1.2.3.4
Source IP Mask......................... 0.0.0.0
Source Layer 4 Operator............... Equal To
Source L4 Port Keyword................. 43
Destination IP Address................. any
TCP Flags............................... FIN (Ignore)
SYN (Set)
RST (Ignore)
PSH (Ignore)
ACK (Ignore)
URG (Ignore)
ACL Hit Count.......................... 43981900

Rule Number: 2
Action................................. permit
Match All.............................. FALSE
Protocol............................... 6(tcp)
Source IP Address..................... any
Destination IP Address............... 1.2.3.4
Destination IP Mask................... 0.0.0.0
TCP Flags......................................................... FIN (Ignore)
SYN (Set)
RST (Ignore)
PSH (Ignore)
ACK (Ignore)
URG (Ignore)

ACL Hit Count.............................................. 1

The following examples show Dynamic ACLs configured for both the data and voice VLAN.

IPv4 Data and Voice:

```bash
console#show ip access-lists
Current number of ACLs: 4 Maximum number of ACLs: 100
ACL Name Rules Count Interface(s) Direction
---------------------- ----- ----- ------------ ---------
IP-DACL-IN-Gi1/0/9#d 1 418 Gi1/0/9 Inbound
IP-VDACL-IN-Gi1/0/9#d 1 0 Gi1/0/9 Inbound
```

IPv6 Data and Voice:

```bash
console#show ipv6 access-lists
Current number of ACLs: 4 Maximum number of ACLs: 100
IPv6 ACL Name Rules Count Interface(s) Direction
---------------------- ------ ----- ------------ ---------
IPV6-DACL-IN-Gi1/0/9#d 1 246 Gi1/0/9 Inbound
IPV6-VDACL-IN-Gi1/0/9#d 1 0 Gi1/0/9 Inbound
```

Display with the ACL name for any of the above (no #d required in command):

```bash
console#show ip access-lists IP-DACL-IN-Gi1/0/9
If ACL Name: IP-DACL-IN-Gi1/0/9#d
Inbound Interface(s):
Gi1/0/9
Rule Number: 50
Action....................................................... permit
Match All.................................................. TRUE
ACL Hit Count............................................. 418
```
show mac access-lists

Use the show mac access-lists command to display a MAC access list and all the rules that are defined for the MAC ACL. Use the [name] parameter to identify a specific MAC ACL to display.

Syntax

show mac access-lists name

- name—Use this parameter to identify the specific MAC ACL to display.

Default Configuration

This command has no default configuration

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The hit counter applies to the ACL, not to the interface. It shows the sum of all matching packets across all interfaces to which the ACL is applied. For an ACL applied to multiple interfaces, the hit counter will be identical for all interfaces.

Command History

Updated in 6.3.0.1 firmware. Updated User Guidelines in 6.3.0.5 firmware.

Example

console#show mac access-lists

Current number of all ACLs: 9 Maximum number of all ACLs: 100

<table>
<thead>
<tr>
<th>MAC ACL Name</th>
<th>Rules</th>
<th>Count</th>
<th>Interface(s)</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELL123</td>
<td>1</td>
<td>0</td>
<td>Gi1/0/1</td>
<td>Inbound</td>
</tr>
<tr>
<td>ipv4-multicast</td>
<td>2</td>
<td>14666</td>
<td>Po1-64,Gi1/0/1-24,</td>
<td>Inbound</td>
</tr>
</tbody>
</table>

console#show mac access-lists mac-acl
MAC ACL Name: mac-acl

Outbound Interface(s):
Gi1/0/8

Rule Number: 1
Action......................................... permit
Source MAC Address......................... 0000.1122.3344
Source MAC Mask.............................. FFFF.0000.0000
EtherType...................................... ipx
VLAN........................................... 100
ACL Hit Count............................... 213

Rule Number: 2
Action......................................... permit
Source MAC Address......................... 0000.1133.2244
Source MAC Mask.............................. FFFF.0000.0000
EtherType...................................... ip
VLAN........................................... 100
ACL Hit Count............................... 213
MAC Address Table Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dell EMC Networking switches implement a MAC Learning Bridge in compliance with IEEE 802.1Q. The switches implement independent VLAN learning (IVL). Dynamically learned MAC addresses are used to filter the set of ports on which a frame is forwarded within a VLAN, that is, the destination MAC address and ingress VLAN for a frame entering the switch is looked up in the MAC address table and, if a match is found, the frame is forwarded out the matching port(s). If no match is found, the frame is flooded out all ports in the VLAN except for the ingress port.

When a frame is received on a port, the source MAC address (and VLAN) is looked up in the MAC address table. If no matching entry is found, a new entry is added to the MAC address table associated with the source port. If a matching entry is found, the matching entry timestamp is refreshed such that it will continue to remain in the MAC address table. Dynamic MAC address entries for which no frames have been received within the aging period are removed out of the MAC address table. The administrator can globally configure the MAC address aging timer.

Administrators can configure static MAC address entries. Static MAC entries are treated in the same manner as dynamic MAC address entries for the purposes of frame forwarding. Static MAC addresses never age out of the MAC address database and can only be removed by administrator action.

Port security allows the administrator to disable learning of MAC addresses on selected interfaces. Dynamically learned MAC addresses are flushed on an interface at the time port security is enabled. The interface then dynamically learns MAC addresses up to the configured limit and no more. The administrator may configure a limit of 0 in order to disable MAC learning on the interface entirely. In this configuration, it is advisable to configure static MAC entries on the interface in order to facilitate forwarding.
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear mac address-table</th>
<th>show mac address-table multicast</th>
<th>show mac address-table dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mac address-table aging-time</td>
<td>show mac address-table dynamic</td>
<td>show mac address-table interface</td>
</tr>
<tr>
<td>clear mac address-table multicast forbidden address</td>
<td>show mac address-table address</td>
<td>show mac address-table static</td>
</tr>
<tr>
<td>mac address-table static</td>
<td>show mac address-table count</td>
<td>show mac address-table vlan</td>
</tr>
<tr>
<td>switchport port-security (Interface Configuration)</td>
<td>show mac address-table count</td>
<td>show port-security</td>
</tr>
</tbody>
</table>

**clear mac address-table**

Use the `clear mac address-table` command to remove learned entries from the forwarding database.

**Syntax**

```
clear mac address-table dynamic [address mac-addr | interface interface-id | vlan vlan-id]
```

- `mac-addr`—Delete the specified MAC address.
- `interface-id`—Delete all dynamic MAC addresses on the specified Ethernet port or port channel.
- `vlan-id`—Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4093.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode
User Guidelines
This command has no user guidelines.

Example
In this example, the mac address-table tables are cleared.

```
console#clear mac address-table dynamic
```

**mac address-table aging-time**

Use the `mac address-table aging-time` command in Global Configuration mode to set the aging time of the address. To restore the default, use the `no` form of the `mac address-table aging-time` command.

**Syntax**

```
mac address-table aging-time {0 | 10-1000000}
no mac address-table aging-time
```

- 0—Disable aging time for the MAC Address Table.
- 10-1000000—Set the number of seconds aging time for the MAC Address Table.

**Default Configuration**

300 seconds

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

In this example the MAC Address Table aging time is set to 400.

```
console(config)#mac address-table aging-time 400
```
**mac address-table multicast forbidden address**

Use the `mac address-table multicast forbidden address` command in Global Configuration mode to forbid adding a specific multicast address to specific ports. To allow the multicast group, use the `no` form of this command.

**Syntax**

```
mac address-table multicast forbidden address vlan vlan-id {mac-multicast-address | ip-multicast-address} {add | remove} interface interface-list
no mac address-table multicast forbidden address vlan vlan-id {mac-multicast-address | ip-multicast-address}
```

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **vlan vlan-id**—A valid vlan-id. (Range 1-4093)
- **mac-multicast-address**—MAC multicast address.
- **ip-multicast-address**—IP multicast address.
- **interface-list**—Specify a comma separated list of interface identifiers, a range of interfaces, or a combination of both. Interface identifiers can be port channel interface identifiers or Ethernet interface identifiers. Embedded blanks are not allowed in the list.

**Default Configuration**

No forbidden addresses are defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Before defining forbidden ports, ensure that the multicast group is registered. Changing an unregistered multicast address to forbidden on an mrouter port will effectively forbid the multicast group on all ports on the switch as it inhibits the source of the multicast group.
Examples

In this example the MAC address 0100.5e02.0203 is forbidden on port 2/0/9 within VLAN 8.

```
console(config)#mac address-table multicast forbidden address vlan 8 0100.5e02.0203 add interface gigabitethernet 2/0/9
```

**mac address-table static**

Use the `mac address table static` command in Global Configuration mode to add a static MAC-layer station source address to the bridge table. To delete the MAC address, use the `no` form of the `mac address table static` command.

**Syntax**

```
mac address-table static mac-addr vlan vlan-id interface interface-id
no mac address-table static mac-addr vlan vlan-id interface-id
```

- **mac-address**—A valid MAC address.
- **vlan-id**—Valid VLAN ID (1-4093).
- **interface-id**—The interface to which the received packet is forwarded. Ethernet interface identifiers and port channel identifiers are valid for this command.

**Default Configuration**

No static addresses are defined. The default mode for an added address is permanent.

**Command Mode**

Global Configuration mode

**User Guidelines**

The MAC address may be a unicast or multicast MAC address. Static MAC addresses are never overridden by dynamically learned addresses. This has implications for protocols like IGMP snooping, where statically configuring the MAC address of a multicast router keeps IGMP snooping from dynamically adding the multicast router to a different port.
The maximum number of static MAC addresses that may be configured on a port is limited by the switchport port-security maximum command. This command may be invoked multiple times with different interfaces (and the same VLAN) when used with a multicast MAC address.

**Example**

The following example adds a permanent static MAC address c2f3.220a.12f4 to the MAC address table.

```
console(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet6/0/1
```

**switchport port-security (Global Configuration)**

Use the `switchport port-security` command in Global Configuration mode to enable port security globally. Use the `no` form of the command to disable port security globally.

**Syntax**

```
switchport port-security
no switchport port-security
```

**Default Configuration**

Port security is disabled by default.

No MAC addresses are learned or configured by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Port security must be enabled globally and on the interface in order to be active on the interface. Disabling port security globally does not remove sticky MAC address configuration from the running-config.
Port security allows the network administrator to secure interfaces by specifying (or learning) the allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally. All other host packets are discarded. Port security operates on access, trunk and general mode ports.

Two methods are used to implement Port MAC locking: dynamic locking and static locking. Static locking further has an optional sticky mode.

Dynamic locking implements a ‘first arrival’ mechanism for MAC locking. The administrator specifies how many dynamic addresses may be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. If the MAC address limit has been reached, the packet is discarded. The administrator can disable dynamic locking (learning) by setting the number of allowable dynamic entries to zero.

When a MAC locking enabled link goes down, all of the dynamically locked addresses are ‘freed.’ When the link is restored, that port can once again learn MAC addresses up to the administrator specified limit.

A dynamically locked MAC address is eligible to be aged out if another packet with that MAC address is not seen within the age-out time. Dynamically locked MAC addresses are also eligible to be relearned on another port if station movement occurs. Statically locked MAC addresses are not eligible for aging. If a packet arrives on a port with a source MAC address that is statically locked on another port, then the packet is discarded.

Static locking allows the administrator to specify a list of host MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with a known source MAC address can be forwarded. Any packets with source MAC addresses that are not configured are discarded. The switch treats this as violation and supports send a SNMP port-security trap.

If the administrator knows the specific MAC address (or addresses) that will be connected to a particular port, she can specify those addresses as static entries. By setting the number of allowable dynamic entries to zero, only packets with a source MAC address matching a MAC address in the static list are forwarded.

To configure static locking only, set the dynamic MAC limit to 0. To configure dynamic locking only, set the static MAC limit to 0.
Sticky mode configuration converts all the existing dynamically learned MAC addresses on an interface to sticky. This means that they will not age out and will appear in the running-config. In addition, new addresses learned on the interface will also become sticky. Note that sticky is not the same as static – the difference is that all sticky addresses for an interface are removed from the running-config when the interface is taken out of sticky mode. Static addresses must be removed from the running-config individually.

Sticky MAC addresses appear in the running-config in the following form:

```
switchport port-security mac-address sticky 0011.2233.4455 vlan 33
```

Statically locked MAC addresses appear in the running-config in the following form:

```
switchport port-security mac-address 0011.2233.4455 vlan 33
```

**Command History**

Updated in 6.3.0.1 firmware.

**Example**

Enable port security/MAC locking globally and on an interface.

```
console(config)#switchport port-security
console(config)#interface gi1/0/3
console(config-if-gi1/0/3)#switchport port-security
```

Enable port security/MAC locking globally and on an interface, enable sticky mode on the interface and convert all dynamic addresses on the interface to sticky.

```
console(config)#switchport port-security
console(config)#interface gi1/0/3
console(config-if-gi1/0/3)#switchport port-security
console(config-if-gi1/0/3)#switchport port-security mac-address sticky
```

Add a statically locked MAC address to trunk port Gi1/0/3 and VLAN 33.

```
console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
console(config-if-Gi1/0/3)#switchport port-security mac-address 0011.2233.4455 vlan 33
```

Add a sticky mode statically locked MAC address to trunk port Gi1/0/3 and VLAN 33.

```
```
Remove a sticky mode MAC address from trunk port Gi1/0/3 and VLAN 33.

Convert all dynamically learned MAC addresses on trunk port gi1/0/3 to sticky MAC addresses and save the running-config so the configuration will persist across reboots.

Convert all sticky MAC addresses on trunk port gi1/0/3 to sticky MAC addresses and save the running-config so the configuration will persist across reboots.

**switchport port-security (Interface Configuration)**

Use the `switchport port-security` command to enable or configure port security (MAC locking) globally. Use the `no` form of the command to disable port security globally.

**Syntax**

```
switchport port-security [mac-address { sticky | [sticky] mac-address vlan {vlan-id}}] {dynamic value | maximum value | violation {protect | shutdown}}
```

```
no switchport port-security [mac-address {sticky | mac-address vlan {vlan-id}}] {dynamic | maximum | violation}
```
• **mac-address** — The static MAC address to be configured on the interface and VLAN.

• **vlan-id** — The VLAN identifier on which to configure the MAC address.

• **dynamic** — Configure the maximum number of dynamic MAC addresses that be be learned on the interface. Setting the dynamic limit to 0 causes all received packets with non-static MAC addresses to be considered as violations.

• **sticky** — Configure a sticky MAC address on the interface. If the sticky parameter not given, a statically locked MAC address is configured on the interface.

• **maximum** — Configure the maximum number of static MAC addresses that may be configured on the interface.

• **violation**—Configure the interface to:
  – **protect**—Protect the interface by discarding MAC frames that are not learned (default) and issuing a log message and a trap.
  – **shutdown**—Protect the interface by error disabling the interface and issuing a log message and a trap.

**Default Configuration**

Port security is disabled by default.

No static or sticky MAC addresses are learned or configured by default.

The default number of dynamic MAC addresses per interface is 600 (300 for the N1500 Series switches). The default number of static MAC addresses per interface is 100.

Both limits are subject to the total MAC address limit supported by the system.

**Command Mode**

Interface (Ethernet and port-channel) Configuration mode.

Interface Range mode - Only when using switchport port-security syntax.
User Guidelines

Port security allows the network administrator to secure interfaces by specifying (or learning) the allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally. All other host packets are discarded. Port security operates on access, trunk and general mode ports.

Two methods are used to implement port security: dynamic locking and static locking. Static locking further has an optional sticky mode.

Dynamic locking implements a ‘first arrival’ mechanism for MAC locking. The administrator specifies how many dynamic addresses may be learned on the secure port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. If the MAC address limit has been reached, the packet is discarded, the MAC address is not learned, and a violation is raised. The administrator can disable dynamic learning by setting the number of allowable dynamic entries to zero. This causes all packets with unknown MAC addresses to be considered as violations.

When a port security enabled link goes down, all of the dynamically learned addresses are removed from the MAC forwarding database. When the link is restored, that port can once again learn MAC addresses up to the administrator specified limit.

A dynamically learned MAC address is eligible to be aged out if another packet with that MAC address is not seen within the age-out time. Dynamically learned MAC addresses are also eligible to be re-learned on another port if station movement occurs.

Static locking allows the administrator to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic learning once the dynamic limit has been reached: only packets with a known source MAC address can be forwarded. Any packets with source MAC addresses that are not configured are discarded. The switch treats this as violation.

If the administrator knows the specific MAC address (or addresses) that will be connected to a particular port, she can specify those addresses as static entries. By setting the number of allowable dynamic entries to zero, only packets with a source MAC address matching a MAC address in the static list are forwarded.
Statically locked MAC addresses are not eligible for aging. If a packet arrives on a port with a source MAC address that is statically locked on another port, then the packet is discarded.

To configure static locking only, set the dynamic MAC limit to 0 and configure the static MAC addresses on the interface. To configure dynamic locking only, set the static MAC limit to 0, and set the appropriate dynamic MAC address limit.

MAC addresses seen on an interface other than the learned or configured MAC addresses and in excess of the limit are considered violations of port security. Trap issuance violation actions can be configured using the `snmp-server enable traps port-security` command. The default action is to log a message and send an SNMP trap. Port security can optionally error disable an interface on which a violation occurs using the `switchport port-security violation shutdown` command. Setting the port to shutdown mode also enables the sending of port-security traps.

Enabling sticky mode configuration converts all the existing dynamically learned MAC addresses on an interface to sticky. It also converts the last violation MAC address to sticky, even if the dynamic limit is set to 0. These MAC addresses will not age out and will appear in the running-config. In addition, new addresses learned on the interface will also become sticky. Note that sticky is not the same as static – the difference is that all sticky addresses for an interface are removed from the running-config when the interface is taken out of sticky mode. Static addresses must be removed from the running-config individually.

Sticky MAC addresses appear in the running-config in the following form:

```
switchport port-security mac-address sticky 0011.2233.4455 vlan 33
```

Statically locked MAC addresses appear in the running-config in the following form:

```
switchport port-security mac-address 0011.2233.4455 vlan 33
```

In order for sticky or static MAC addresses to survive a reboot, the configuration must be saved.

Port security must be enabled globally and on the interface in order to be active.

Port security should only be enabled on access mode ports and not on trunk mode ports. This recommendation is not enforced by the switch.
**Command History**

Updated in 6.3.0.1 firmware.

**Example**

Enable port security/MAC locking globally and on an interface.

```plaintext
console(config)#switchport port-security
console(config)#interface gi1/0/3
console(config-if-gi1/0/3)#switchport port-security
```

Enable port security/MAC locking globally and on an interface, enable sticky mode on the interface and convert all dynamic addresses on the interface to sticky.

```plaintext
console(config)#switchport port-security
console(config)#interface gi1/0/3
console(config-if-gi1/0/3)#switchport port-security
console(config-if-gi1/0/3)#switchport port-security mac-address sticky
```

Add a statically locked MAC address to trunk port Gi1/0/3 and VLAN 33.

```plaintext
console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
console(config-if-Gi1/0/3)#switchport port-security mac-address 0011.2233.4455 vlan 33
```

Add a sticky mode statically locked locked MAC address to trunk port Gi1/0/3 and VLAN 33.

```plaintext
console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
console(config-if-Gi1/0/3)#switchport port-security mac-address sticky 0011.2233.4455 vlan 33
```

Remove a sticky mode MAC address from trunk port Gi1/0/3 and VLAN 33.

```plaintext
console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
console(config-if-Gi1/0/3)#no switchport port-security mac-address 0011.2233.4455 vlan 33
```

Convert all dynamically learned MAC addresses on trunk port 33 to sticky MAC addresses and save the running-config so the configuration will persist across reboots.

```plaintext
console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
```
console(config-if-Gi1/0/3)#switchport port-security mac-address sticky
console(config)#do write

Convert all sticky MAC addresses on trunk port 33 to sticky MAC addresses and save the running-config so the configuration will persist across reboots.

console(config)#vlan 33
console(config-vlan33)#interface gi1/0/3
console(config-if-Gi1/0/3)#switchport mode trunk
console(config-if-Gi1/0/3)#switchport port-security mac-address sticky
console(config)#do write

show mac address-table multicast

Use the `show mac address-table multicast` command to display multicast MAC address table information.

**Syntax**

```
show mac address-table multicast [count] | [[vlan vlan-id] [address {mac-multicast-address | ip-multicast-address}] [format {ip | mac}]]
```

- **vlan-id** — A valid VLAN ID value.
- **mac-multicast-address** — A valid MAC multicast address.
- **ip-multicast-address** — A valid IP multicast address.
- **format** — Multicast address display format. Can be **ip** or **mac**.

**Default Configuration**

If format is unspecified, the default is **mac**.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The count parameter requests the display of the address table usage. No other parameters may be supplied with the count parameter. The **address** parameter indicates that the entry matching the specified address is displayed. The **vlan** parameter requests display of entries associated with the specified VLAN. The **format** parameter requests that addresses be displayed
in the specified format. The vlan, address, and format parameters may all be specified together.
A MAC address can be displayed in IP format only if it is in the range 01:00:5e:00:00:00 through 01:00:5e:7f:ff:ff.
Static multicast MAC addresses can be added via the mac address-table static command.

**Example**
In this example, multicast MAC address table information is displayed.

```
console#show mac address-table multicast
Vlan      MAC Address         Type     Ports
-----   -------------------  -------   ------------------
1         0100.5E05.0505      Static

Forbidden ports for multicast addresses:

Vlan      MAC Address                Ports
-----  -----------------------  ---------------------------
1       0100.5E05.0505
```

**NOTE:** A multicast MAC address maps to multiple IP addresses, as shown above.

**Command History**
The description was updated in the 6.4 release.

**show mac address-table**
Use the show mac address-table command in User Exec or Privileged Exec mode to display all entries in the bridge-forwarding database.

**Syntax**
show mac address-table

**Default Configuration**
This command has no default configuration.
**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Use the `show mac address-table multicast` to display multicast MAC address entries along with forbidden multicast MAC entries.

**Example**

In this example, all classes of entries in the mac address-table are displayed.

```
console#show mac address-table
```

Aging time is 300 Sec

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>001E.C9AA.AE19</td>
<td>Management</td>
<td>CPU Interface</td>
</tr>
<tr>
<td>1</td>
<td>001E.C9AA.AC19</td>
<td>Dynamic</td>
<td>Gi1/0/21</td>
</tr>
<tr>
<td>1</td>
<td>001E.C9AA.AE1B</td>
<td>Management</td>
<td>V11</td>
</tr>
<tr>
<td>10</td>
<td>001E.C9AA.AE1B</td>
<td>Management</td>
<td>V110</td>
</tr>
<tr>
<td>90</td>
<td>001E.C9AA.AE1B</td>
<td>Management</td>
<td>V190</td>
</tr>
</tbody>
</table>

Total MAC Addresses in use: 5

**show mac address-table address**

Use the `show mac address-table address` command in User Exec or Privileged Exec mode to display all entries in the bridge-forwarding database for the specified MAC address.

**Syntax**

```
show mac address-table address mac-address [interface interface-id] [vlan vlan-id]
```

- `mac-address`—A MAC address.
- `interface-id`—Display information for a specific interface. Valid interfaces include Ethernet ports and port channels.
- `vlan-id`—Display entries for the specific VLAN only. The range is 1 to 4093.
Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all
Configuration submodes

User Guidelines
This command has no user guidelines.

Example
In this example, the mac address table entry for 0000.E26D.2C2A is
displayed.

console#show mac address-table address 0000.E26D.2C2A

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.E26D.2C2A</td>
<td>Dynamic</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

show mac address-table count
Use the show mac address-table count command in User Exec or Privileged
Exec mode to display the number of addresses present in the Forwarding
Database.

Syntax
show mac address-table count [vlan vlan-id | interface interface-id]

- interface-id—Specify an interface type; valid interfaces include Ethernet
  ports and port channels.
- vlan-id—Specify a valid VLAN, the range is 1 to 4093.

Default Configuration
This command has no default configuration.
**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the addresses in the Forwarding Database:

```plaintext
console#show mac address-table count
Capacity: 8192
Used: 109
Static addresses: 2
Secure addresses: 1
Dynamic addresses: 97
Internal addresses: 9
```

**show mac address-table dynamic**
Use the `show mac address-table` command in User Exec or Privileged Exec mode to display all dynamic entries in the bridge-forwarding database.

**Syntax**
```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id]
```
- mac-address—A MAC address.
- interface-id —Display information for a specific interface. Valid interfaces include Ethernet ports and port channels.
- vlan-id—Display entries for the specific VLAN only. The range is 1 to 4093.

**Default Configuration**
This command has no default configuration.
**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

In this example, all dynamic entries in the mac address-table are displayed.

```console
console#show mac address-table dynamic
Aging time is 300 Sec
Vlan  Mac Address    Type    Port
----- -------------- ------- --------------
  1    0000.0001.0000 Dynamic Gi1/0/1
  1    0000.8420.5010 Dynamic Gi1/0/1
  1    0000.E26D.2C2A Dynamic Gi1/0/1
  1    0000.E89A.596E Dynamic Gi1/0/1
  1    0001.02F1.0B33 Dynamic Gi1/0/1
```

**show mac address-table interface**

Use the `show mac address-table` command in User Exec or Privileged Exec mode to display all entries in the mac address-table.

**Syntax**

```
show mac address-table interface interface-id [vlan vlan-id]
```

- **interface-id** — Specify an interface type. Valid interfaces include Ethernet ports and port channels.
- **vlan-id** — Specify a valid VLAN. The range is 1 to 4093.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
In this example, all classes of entries in the bridge-forwarding database for Gigabit Ethernet interface 1/0/1 are displayed.

```
console#show mac address-table interface gigabitethernet 1/0/1
Aging time is 300 Sec
Vlan Mac Address    Type    Port
---- -------------- ----    -------------
1    0000.0001.0000 Dynamic Gi1/0/1
1    0000.8420.5010 Dynamic Gi1/0/1
1    0000.E26D.2C2A Dynamic Gi1/0/1
1    0000.E89A.596E Dynamic Gi1/0/1
1    0001.02F1.0B33 Dynamic Gi1/0/1
```

**show mac address-table static**

Use the `show mac address-table static` command in User Exec or Privileged Exec mode to display static entries in the bridge-forwarding database.

**Syntax**

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id]
```

- `mac-address` — A MAC address.
- `interface-id` — Specify an interface type; valid interfaces include Ethernet ports and port channels.
- `vlan-id` — Specify a valid VLAN; the range is 1 to 4093.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
In this example, all static entries in the bridge-forwarding database are displayed.

console#show mac address-table static

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0001.0001.0001</td>
<td>Static</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

show mac address-table vlan

Use the show mac address-table vlan command in User Exec or Privileged Exec mode to display all entries in the bridge-forwarding database for the specified VLAN.

Syntax
show mac address-table [vlan vlan-id]

• vlan-id—Specify a valid VLAN; the range is 1 to 4093.

Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
In this example, multiple classes of entries in the bridge forwarding database are displayed.

console(config-if-Gi1/0/4)#show mac address-table vlan 1
Aging time is 400 Sec

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1418.7715.1BAA</td>
<td>Dynamic</td>
<td>Gi2/0/29</td>
</tr>
<tr>
<td>1</td>
<td>1418.7715.47E8</td>
<td>Management</td>
<td>CPU</td>
</tr>
<tr>
<td>1</td>
<td>2047.47BA.F696</td>
<td>Dynamic</td>
<td>Gi2/0/29</td>
</tr>
<tr>
<td>1</td>
<td>B8CA.3AD5.DF1A</td>
<td>Static</td>
<td>Gi2/0/29</td>
</tr>
</tbody>
</table>

**show port-security**

Use the `show ports security` command to display port security (MAC locking) configuration.

**Syntax**

`show port-security [ interface-id | all | dynamic interface-id | static interface-id | violation interface-id ]`

- interface-id —An Ethernet or port channel interface identifier.
- all—Display information for all interfaces.

**Default Configuration**

Port security is disabled by default.

No port security MAC addresses are learned or configured by default.

The maximum static MAC address limit is 100 MAC addresses.

The maximum dynamic MAC address limit is 600 MAC addresses.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Setting the dynamic limit to 0 causes all received packets with non-static or sticky MAC addresses to be considered as violations.

This information is shown if no parameters are given:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>The configured global administrative status of port MAC locking.</td>
</tr>
</tbody>
</table>

This information is shown if only an interface parameter is given:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Identifier</td>
<td>The interface identifier.</td>
</tr>
<tr>
<td>Status</td>
<td>The port security administrative status (enabled/disabled).</td>
</tr>
<tr>
<td>Max-dynamic</td>
<td>The dynamic MAC address limit.</td>
</tr>
<tr>
<td>Max-static</td>
<td>The static address limit.</td>
</tr>
<tr>
<td>Protect</td>
<td>Trap issued on violation (enabled/disabled).</td>
</tr>
<tr>
<td>Frequency</td>
<td>The frequency of trap issuance (in seconds).</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shut down (err-disable) interface on violation (enabled/disabled).</td>
</tr>
<tr>
<td>Sticky Mode</td>
<td>Sticky mode configuration (enabled/disabled).</td>
</tr>
</tbody>
</table>

This information is shown if the dynamic parameter is given:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamically Learned MAC Address</td>
<td>Dynamically learned MAC addresses.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN on which the MAC address is learned.</td>
</tr>
</tbody>
</table>

This information is shown if the static parameter is given:
This information is shown if the violation parameter is given:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>Statically configured MAC addresses.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier of the MAC address.</td>
</tr>
<tr>
<td>Sticky</td>
<td>Indicates if the secure MAC address is sticky.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>The source MAC address of the last packet discarded on the interface. These are packets with unknown MAC addresses, e.g., as in the case of the dynamic limit set to 0.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier of the discarded packet, if applicable.</td>
</tr>
</tbody>
</table>

**Command History**
Updated in 6.3.0.1 firmware.

**Example**

```
console(config)#show port-security static gi1/0/1
```

Number of static MAC addresses configured: 2

<table>
<thead>
<tr>
<th>Static MAC address</th>
<th>VLAN ID</th>
<th>Sticky</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:ad:32:01</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>00:10:fe:48:19</td>
<td>2</td>
<td>No</td>
</tr>
</tbody>
</table>
Auto-VoIP Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Voice over Internet Protocol (VoIP) allows network users to make telephone calls using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration ensures high-quality application performance. The Auto-VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS. The Auto-VoIP service is independent of the Voice VLAN service. Only one of the two services should be deployed in any network.

The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. The Auto VoIP module provides the capability to assign the highest priority for the following VoIP packets:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

Auto-VoIP borrows ACL lists from the global system pool. ACL lists allocated by Auto-VoIP reduce the total number of ACLs available for use by the network operator. Enabling Auto-VoIP uses one ACL list to monitor for VoIP sessions. Each monitored VoIP session utilizes two rules from an additional ACL list. This means that the maximum number of ACL lists allocated by Auto-VoIP is two. The Auto-VoIP feature limits the maximum number of simultaneous users to 16. Administrators should utilize the Voice VLAN feature for deployment of IP voice service in an enterprise network because Voice VLAN scales to significantly higher numbers of users.

NOTE: This feature is not available on the N3000 when loaded with the AGGREGATION ROUTER enabled firmware (e.g., N3000_BGPvA.B.C.D.stk).

Commands in this Section

This section explains the following commands:
show switchport voice

Use the show switchport voice command to show the status of Auto-VoIP on an interface or all interfaces.

Syntax

show switchport voice [ interface-id ]

- interface-id —An Ethernet or port channel interface identifier.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

See the debug auto-voip command for assistance in troubleshooting Auto-VoIP issues.

This command accepts an Ethernet interface identifier or a port channel identifier.

Examples

The following example shows command output when a port is not specified:

console#show switchport voice

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Disabled</td>
<td>6</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Disabled</td>
<td>6</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Disabled</td>
<td>6</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Disabled</td>
<td>6</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Disabled</td>
<td>6</td>
</tr>
</tbody>
</table>
The following example shows command output when a port is specified:

```
console#show switchport voice gigabitethernet 1/0/1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Disabled</td>
<td>6</td>
</tr>
</tbody>
</table>

The command output provides the following information:

- **AutoVoIP Mode**—The Auto VoIP mode on the interface.
• Traffic Class—The Cos Queue or Traffic Class to which all VoIP traffic is mapped. This is not configurable and defaults to the highest COS queue available in the system for data traffic.

switchport voice detect auto

The switchport voice detect auto command is used to enable the VoIP Profile on all the interfaces of the switch (global configuration mode) or for a specific interface (interface configuration mode). Use the no form of the command to disable the VoIP Profile.

Syntax

switchport voice detect auto

no switchport voice detect auto

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The switch Auto-VoIP capability is independent of the Voice VLAN capability. Voice VLAN configuration has no effect on the Auto-VoIP capabilities. Voice VLAN is recommended for enterprise deployments as Auto-VoIP is limited in the number of active VoIP users that can be serviced.

This command is valid for Ethernet and port channel interfaces.

Example

console(config)#interface tengigabitethernet 1/0/1
console(config-if-Tel/0/1)#switchport voice detect auto
Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol which inter-operates with Cisco network equipment and is used to share information between neighboring devices. Dell EMC Networking switches participate in the ISDP protocol and are able to both discover and be discovered by devices that support the Cisco Discovery Protocol (CDP). ISDP is based on CDP, which is a precursor to LLDP.

Commands in this Section
This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isdp counters</td>
<td>show isdp</td>
</tr>
<tr>
<td>clear isdp table</td>
<td>show isdp entry</td>
</tr>
<tr>
<td>isdp advertise-v2</td>
<td>show isdp interface</td>
</tr>
<tr>
<td>isdp enable</td>
<td>show isdp neighbors</td>
</tr>
<tr>
<td>isdp holdtime</td>
<td>show isdp traffic</td>
</tr>
<tr>
<td>isdp timer</td>
<td></td>
</tr>
</tbody>
</table>

**clear isdp counters**
The `clear isdp counters` command clears the ISDP counters.

**Syntax**
clear isdp counters

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode
User Guidelines
There are no user guidelines for this command.

Example
console#clear isdp counters

clear isdp table
The clear isdp table command clears entries in the ISDP table.

Syntax
clear isdp table

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode

User Guidelines
There are no user guidelines for this command.

Example
console#clear isdp table

isdp advertise-v2
The isdp advertise-v2 command enables the sending of ISDP version 2 packets from the device. Use the no form of this command to send version 1 packets.

Syntax
isdp advertise-v2
no isdp advertise-v2
Default Configuration
ISDP sends version 2 packets by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)#isdp advertise-v2

isdp enable
The isdp enable command enables ISDP on the switch. User the “no” form of this command to disable ISDP. Use this command in global configuration mode to enable the ISDP function on the switch. Use this command in interface mode to enable sending ISDP packets on a specific interface.

Syntax
isdp enable
no isdp enable

Default Configuration
ISDP is enabled.

Command Mode
Global Configuration mode.
Interface Configuration (Ethernet) mode.

User Guidelines
There are no user guidelines for this command.

Example
The following example enables isdp on interface Gi1/0/1.
Layer 2 Switching Commands

isdp holdtime

The isdp holdtime command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds. Use the no form of this command to reset the holdtime to the default.

Syntax

isdp holdtime time
no isdp holdtime

• time—The time in seconds (range 10–255 seconds).

Default Configuration

The default holdtime is 180 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command specifies the amount of time the partner device should maintain the ISDP information. The local device uses the hold time in packets received from the partner device. Configuring the hold time locally does not change the amount of time displayed by the show isdp command. Configure the hold time on the partner device to change the amount of time the switch maintains the partner information.

Example

The following example sets isdp holdtime to 40 seconds.

console(config)#isdp holdtime 40
**isdp timer**

The `isdp timer` command sets period of time between sending new ISDP packets. The range is given in seconds. Use the “no” form of this command to reset the timer to the default.

**Syntax**

`isdp timer time`

`no isdp timer`

- **time**—The time in seconds (range: 5–254 seconds).

**Default Configuration**

The default timer is 30 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

Configuring the timer to a low value on a large number interfaces may affect system processing due to CPU overload. Use the `show process cpu` command to examine the system load.

**Example**

The following example sets the `isdp timer` value to 40 seconds.

```
console(config)#isdp timer 40
```

**show isdp**

The `show isdp` command displays global ISDP settings.

**Syntax**

`show isdp`

**Default Configuration**

There is no default configuration for this command.
Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show isdp
Timer.............................. 30
Hold Time.......................... 180
Version 2 Advertisements........... Enabled
Neighbors table last time changed... 0 days 00:06:01
Device ID.......................... QTFMFPW82400020
Device ID format capability........ Serial Number
Device ID format.................. Serial Number

show isdp entry
The show isdp entry command displays ISDP entries. If a device id specified, then only the entry about that device is displayed.

Syntax
show isdp entry {all | deviceid}

• all—Show ISDP settings for all devices.
• deviceid—The device ID associated with a neighbor.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.
Example

console#show isdp entry Switch

Device ID: N2000/N3000 Series Switch
Address(es):
  IP Address: 172.20.1.18
  IP Address: 172.20.1.18
Capability: Router IGMP
Platform: cisco WS-C4948
Interface: Gi1/0/1
Port ID: Gi1/0/1
Native VLAN: 234
Holdtime: 64
Advertisement Version: 2
Entry last changed time: 0 days 00:13:50
Version:
Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000 I9K91S-M),
Version 12.2(25)EWA9, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 21-Mar-07 12:20 by tinhuang

show isdp interface

The show isdp interface command displays ISDP settings for the specified interface.

Syntax

show isdp interface {all | interface-id}

  - interface-id—An Ethernet interface identifier.
  - all—Display all interfaces.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command accepts an Ethernet interface identifier.

Example
console#show isdp interface all

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

console#show isdp interface gigabitethernet 1/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

show isdp neighbors
The show isdp neighbors command displays the list of neighboring devices.

Syntax
show isdp neighbors [interface-id][detail]
  • interface-id—A Ethernet interface identifier.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

The information displayed varies based upon the information received from the ISDP neighbor.

**Example**

```
console#show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID                Intf      Holdtime  Capability Platform         Port ID
------------------------ --------- --------- ---------- ---------------- ---------
CN0H784T2829841E0534A00  Gi1/0/13  163       R          N3048            Gi1/0/13
R3                       Gi1/0/16  157       R          N3048            Gi1/0/16

console#show isdp neighbors detail

Device ID                  Switch
Address(es):
  IP Address:                 172.20.1.18
  IP Address:                 172.20.1.18
Capability                 Router IGMP
Platform                    cisco WS-C4948
Interface                   Gi1/0/1
Port ID                     GigabitEthernet1/1
Native VLAN                 234
Holdtime                    162
Advertisement Version      2
Entry last changed time     0 days 00:55:20
Version:
Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-19K91S-M), Version 12.2(25)EWA9, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 21-Mar-07 12:20 by tinhuang
```

**show isdp traffic**

The `show isdp traffic` command displays ISDP statistics.

**Syntax**

```
show isdp traffic
```

**Default Configuration**

There is no default configuration for this command.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show isdp traffic

ISDP Packets Received......................... 4253
ISDP Packets Transmitted....................... 127
ISDPv1 Packets Received........................ 0
ISDPv1 Packets Transmitted..................... 0
ISDPv2 Packets Received......................... 4351
ISDPv2 Packets Transmitted..................... 4253
ISDP Bad Header................................ 0
ISDP Checksum Error............................ 0
ISDP Transmission Failure...................... 0
ISDP Invalid Format............................ 0
ISDP Table Full................................ 392
ISDP Ip Address Table Full..................... 737
```
DHCP Layer 2 Relay Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

In the majority of network configurations, DHCP clients and their associated servers do not reside on the same IP network or subnet. Therefore, some kind of third-party agent is required to transfer DHCP messages between clients and servers. Such an agent is known as a DHCP Relay agent.

The DHCP Relay agent accepts DHCP requests from any routed interface, including VLANs. The agent relays requests from a subnet without a DHCP server to a server or next-hop agent on another subnet. Unlike a router which switches IP packets transparently, a DHCP Relay agent processes DHCP messages and generates new DHCP messages as a result.

The Dell EMC Networking DHCP Relay supports DHCP Option 82 circuit-id and remote-id for a VLAN.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp l2relay (Global Configuration)</td>
<td>show dhcp l2relay stats interface</td>
</tr>
<tr>
<td>dhcp l2relay (Interface Configuration)</td>
<td>–</td>
</tr>
<tr>
<td>dhcp l2relay circuit-id</td>
<td>show dhcp l2relay agent-option vlan</td>
</tr>
<tr>
<td>dhcp l2relay remote-id</td>
<td>show dhcp l2relay vlan</td>
</tr>
<tr>
<td>dhcp l2relay trust</td>
<td>show dhcp l2relay circuit-id vlan</td>
</tr>
<tr>
<td>dhcp l2relay vlan</td>
<td>show dhcp l2relay remote-id vlan</td>
</tr>
<tr>
<td>show dhcp l2relay all</td>
<td>clear dhcp l2relay statistics interface</td>
</tr>
<tr>
<td>show dhcp l2relay interface</td>
<td>–</td>
</tr>
</tbody>
</table>
**dhcp l2relay (Global Configuration)**

Use the `dhcp l2relay` command to enable Layer 2 DHCP Relay functionality. The subsequent commands mentioned in this section can only be used when the L2-DHCP Relay is enabled. Use the `no` form of this command to disable L2-DHCP Relay.

**Syntax**

dhcp l2relay
no dhcp l2relay

**Default Configuration**

DHCP L2 Relay is disabled by default.

**Command Mode**

Global Configuration.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config)#dhcp l2relay
```

**dhcp l2relay (Interface Configuration)**

Use the `dhcp l2relay` command to enable DHCP L2 Relay for an interface. Use the `no` form of this command to disable DHCP L2 Relay for an interface.

**Syntax**

dhcp l2relay
no dhcp l2relay

**Default Configuration**

DHCP L2 Relay is disabled on all interfaces by default.
**Command Mode**  
Interface Configuration (Ethernet, Port-channel).

**User Guidelines**  
There are no user guidelines for this command.

**Example**  
```
console(config-if-Gi1/0/1)#dhcp l2relay
```

**dhcp l2relay circuit-id**  
Use the `dhcp l2relay circuit-id` command to enable setting the DHCP Option 82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82. Use the `no` form of this command to disable setting the DHCP Option 82 Circuit ID.

**Syntax**  
```
dhcp l2relay circuit-id vlan vlan-list
no dhcp l2relay circuit-id vlan vlan-list
```

- `vlan-list` — A list of VLAN IDs. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

**Default Configuration**  
Setting the DHCP Option 82 Circuit ID is disabled by default.

**Command Mode**  
Global Configuration

**User Guidelines**  
There are no user guidelines for this command.

**Example**  
```
console(config)#dhcp l2relay circuit-id vlan 340-350
```
**dhcp l2relay remote-id**

Use the `dhcp l2relay remote-id` command to enable setting the DHCP Option 82 Remote ID for a VLAN. When enabled, the supplied string is used for the Remote ID in DHCP Option 82. Use the `no` form of this command to disable setting the DHCP Option 82 Remote ID.

**Syntax**

dhcp l2relay remote-id remoteId vlan vlan-list  
no dhcp l2relay remote-id vlan vlan-list

- remoteId—The string to be used as the remote ID in the Option 82 (Range: 1 - 128 characters).
- vlan-list—A list of VLAN IDs. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

**Default Configuration**

Setting the DHCP Option 82 Remote ID is disabled by default.

**Command Mode**

Global Configuration.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config)#dhcp l2relay remote-id dslforum vlan 10,20-30
```

**dhcp l2relay trust**

Use the `dhcp l2relay trust` command to configure an interface to mandate Option-82 on receiving DHCP packets.

**Syntax**

dhcp l2relay trust  
no dhcp l2relay trust
Default Configuration
DHCP Option 82 is discarded by default.

Configuration Mode
Interface Configuration (Ethernet, Port-channel).

User Guidelines
There are no user guidelines for this command.

Example
console(config-if-Gi1/0/1)#dhcp l2relay trust

dhcp l2relay vlan
Use the dhcp l2relay vlan command to enable the L2 DHCP Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing. Use the no form of this command to disable L2 DHCP Relay for a set of VLANs.

Syntax
dhcp l2relay vlan vlan-list
no dhcp l2relay vlan vlan-list

- vlan-list— A list of VLAN IDs. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

Default Configuration
DHCP L2 Relay is disabled on all VLANs by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.
Example
console(config)#dhcp l2relay vlan 10,340-345

**show dhcp l2relay all**

Use the `show dhcp l2relay all` command to display the summary of DHCP L2 Relay configuration.

**Syntax**

`show dhcp l2relay all`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```console
console #show dhcp l2relay all
DHCP L2 Relay is Enabled.
Interface   L2RelayMode  TrustMode
----------  -----------  -----------
Gi1/0/2     Enabled      untrusted
Gi1/0/4     Disabled     trusted
VLAN Id   L2 Relay    CircuitId   RemoteId
--------- ----------  ----------- ------------
3           Disabled    Enabled    --NULL--
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    --dell--
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```
**show dhcp l2relay interface**

Use the `show dhcp l2relay interface` command to display DHCP L2 Relay configuration specific to interfaces.

**Syntax**

```
show dhcp l2relay interface {all | interface-id}
```

- `all`—Show all interfaces.
- `interface-id`—Show the specified interface information. The interface may be an Ethernet interface or a port-channel.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Command History**

Port-channel capability added in version 6.5 firmware.

**Example**

```
console#show dhcp l2relay interface all
DHCP L2 Relay is Enabled.
Interface   L2RelayMode  TrustMode
-----------  -----------  --------------
0/2          Enabled     untrusted
0/4          Disabled    trusted
```

**show dhcp l2relay stats interface**

Use the `show dhcp l2relay stats interface` command to display DHCP L2 Relay statistics specific to interfaces.
Syntax

show dhcp l2relay stats interface {all | interface-id}

- all—Show all interfaces.
- interface-id—An Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

There are no user guidelines for this command.

Example

cconsole#show dhcp l2relay stats interface all

DHCP L2 Relay is Enabled.

<table>
<thead>
<tr>
<th>Interface</th>
<th>UntrustedServer</th>
<th>UntrustedClient</th>
<th>TrustedServer</th>
<th>TrustedClient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MsgsWithOpt82</td>
<td>MsgsWithoutOpt82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show dhcp l2relay agent-option vlan

Use the show dhcp l2relay agent-option vlan command to display DHCP L2 Relay Option-82 configuration specific to VLANs.

Syntax

show dhcp l2relay agent-option vlan vlan-list

- vlan-list—Show information for the specified VLAN range. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)
**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console# show dhcp l2relay agent-option vlan 5-10
DHCP L2 Relay is Enabled.
VLAN Id L2 Relay CircuitId RemoteId
--------- ----------  ----------- ------------
 5       Enabled     Enabled    --NULL--
 6       Enabled     Enabled    broadcom
 7       Enabled     Disabled   --NULL--
 8       Enabled     Disabled   --NULL--
 9       Enabled     Disabled   --NULL--
10      Enabled     Disabled   --NULL--
```

**show dhcp l2relay vlan**

Use the `show dhcp l2relay vlan` command to display whether DHCP L2 Relay is globally enabled on the specified VLAN or VLAN range.

**Syntax**

```
show dhcp l2relay vlan vlan-list

• vlan-list—Show information for the specified VLAN range. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)
```

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show dhcp l2relay vlan 100
DHCP L2 Relay is Enabled.
DHCP L2 Relay is enabled on the following VLANs:
  100
```

**show dhcp l2relay circuit-id vlan**
Use the `show dhcp l2relay circuit-id vlan` command to display whether DHCP L2 Relay is globally enabled and whether the DHCP Circuit-ID option is enabled on the specified VLAN or VLAN range.

**Syntax**
```
show dhcp l2relay circuit-id vlan vlan-list
```
- `vlan-list`—Show information for the specified VLAN range. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show dhcp l2relay circuit-id vlan 300
```
DHCP L2 Relay is Enabled.
DHCP Circuit-Id option is enabled on the following VLANs:

show dhcp l2relay remote-id vlan

Use the show dhcp l2relay remote-id vlan command to display whether DHCP L2 Relay is globally enabled and shows the remote ID configured on the specified VLAN or VLAN range.

Syntax

show dhcp l2relay remote-id vlan vlan-list

- vlan-list—Show information for the specified VLAN range. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

There are no user guidelines for this command.

Example

console#show dhcp l2relay remote-id vlan 200
DHCP L2 Relay is Enabled.
VLAN ID   Remote Id
--------   ------------
200   remote_22

clear dhcp l2relay statistics interface

Use the show dhcp l2relay statistics interface command to reset the DHCP L2 Relay counters to zero. Specify the port with the counters to clear, or use the all keyword to clear the counters on all ports.
Syntax

clear dhcp l2relay statistics interface {all | interface-id}

• all—Show all interfaces.
• interface-id—An Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

There are no user guidelines for this command.

Example

console#clear dhcp l2relay statistics interface gi1/0/1
DHCP Snooping Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

DHCP Snooping is a security feature that monitors DHCP messages between DHCP clients and DHCP server to filter harmful DHCP messages and build a bindings database of {MAC address, IP address, VLAN ID, interface} tuples that are considered authorized.

The DHCP snooping application processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. When there is a mismatch, DHCP snooping logs and drops the packet.

DHCP Snooping forwards valid client messages on trusted members within the VLAN. If DHCP Relay and/or DHCP Server coexist with DHCP Snooping, the DHCP client message is sent to the DHCP Relay or/and DHCP Server for further processing.

The DHCP Snooping application uses DHCP messages to build and maintain the binding's database. The binding's database only includes data for clients on untrusted ports. DHCP Snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP Snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP Snooping removes bindings in response to DECLINE, RELEASE, and NACK messages.

The DHCP Snooping application ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports. The network administrator can enter static bindings into the binding database.

IP Source Guard and Dynamic ARP Inspection use the DHCP Snooping bindings database for the validation of IP and ARP packets.
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip dhcp snooping binding</td>
</tr>
<tr>
<td>clear ip dhcp snooping statistics</td>
</tr>
<tr>
<td>ip dhcp snooping</td>
</tr>
<tr>
<td>ip dhcp snooping binding</td>
</tr>
<tr>
<td>ip dhcp snooping database</td>
</tr>
<tr>
<td>ip dhcp snooping database write-delay</td>
</tr>
<tr>
<td>ip dhcp snooping limit</td>
</tr>
<tr>
<td>ip dhcp snooping log-invalid</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
</tr>
<tr>
<td>ip dhcp snooping verify mac-address</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
</tr>
<tr>
<td>show ip dhcp snooping database</td>
</tr>
<tr>
<td>show ip dhcp snooping database write-delay</td>
</tr>
<tr>
<td>show ip dhcp snooping interfaces</td>
</tr>
<tr>
<td>show ip dhcp snooping statistics</td>
</tr>
<tr>
<td>show ip dhcp snooping statistics</td>
</tr>
</tbody>
</table>

clear ip dhcp snooping binding

Use the clear ip dhcp snooping binding command to clear all DHCP Snooping bindings on a specific interface or on all interfaces.

Syntax

```
clear ip dhcp snooping binding {* | interface interface-id}
```

- `*`—Clear all DHCP Snooping entries.
- `interface interface-id`—Clear all DHCP Snooping entries on the specified interface. The interface may be an Ethernet interface or a port-channel.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec

User Guidelines

There are no user guidelines for this command.
**Command History**
Port-channel capability added in version 6.5 firmware.

**clear ip dhcp snooping statistics**
Use the `clear ip dhcp snooping statistics` command to clear all DHCP Snooping statistics.

**Syntax**
clear ip dhcp snooping statistics

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec

**User Guidelines**
There are no user guidelines for this command.

**Example**
console#clear ip dhcp snooping statistics

**ip dhcp snooping**
Use the `ip dhcp snooping` command to enable DHCP snooping globally, or on a range of VLANs. Use the “no” form of this command to disable DHCP snooping.

**Syntax**
ip dhcp snooping [vlan vlan-list]

no ip dhcp snooping

**Default Configuration**
DHCP Snooping is globally disabled by default. DHCP Snooping is not enabled on any VLAN by default.
**Command Mode**
Global Configuration mode

**User Guidelines**
To enable DHCP snooping, do the following:
1. Enable DHCP Snooping globally.
2. Enable DHCP Snooping per VLAN.
3. Configure at least one DHCP Snooping trusted port via which the DHCP server may be reached.

The bindings database populated by DHCP snooping is used by several other services, including IP source guard and dynamic ARP inspection. DHCP snooping must be enabled for these services to operate.

**Example**
The following configuration enables DHCP snooping on VLAN 1 for a switch connected to a DHCP server over interface gi1/0/4:

```
cfg@switch(config)#ip dhcp snooping
console(config)#ip dhcp snooping vlan 1
console(config-if-vlan1)#exit
console(config)#interface gi1/0/4
console(config-if-Gi1/0/4)#ip dhcp snooping trust
```

**ip dhcp snooping binding**
Use the `ip dhcp snooping binding` command to configure a static DHCP Snooping binding. Use the “no” form of this command to remove a static binding.

**Syntax**

```
ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id
no ip dhcp snooping binding mac-address
```

- **mac-address**—The client’s MAC address.
- **vlan-id**—The identifier of the VLAN the client is authorized to use.
- **ip-address**—The IP address of the client.
- **interface-id**—The interface on which the client is authorized. The interface may be an Ethernet interface identifier or a port channel interface identifier.

**Default Configuration**
There are no static or dynamic DHCP snooping bindings by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config)#ip dhcp snooping binding 00:00:00:00:00:01 vlan 10
10.131.12.134 interface Gi1/0/1
```

**ip dhcp snooping database**
Use the **ip dhcp snooping database** command to configure the persistent storage location of the DHCP snooping database. This can be local to the switch or on a remote machine.

**Syntax**
```
ip dhcp snooping database {local | tftp://hostIP/filename}
```
- **hostIP**—The IP address of the remote host.
- **filename**—The name of the file for the database on the remote host. The filename may contain any printable character except a question mark and is checked only when attempting to open the file. The file must reside in the working directory of the TFTP server. Specification of a sub-directory in the file name parameter is not supported.

**Default Configuration**
The database is stored locally by default.

**Configuration Mode**
Global Configuration mode.
User Guidelines
There are no user guidelines for this command.

Example
The following example configures the storage location of the snooping database as local.

console(config)#ip dhcp snooping database local

The following example configures the storage location of the snooping database as remote.

console(config)#ip dhcp snooping database tftp://10.131.11.1/db.txt

ip dhcp snooping database write-delay

Use the `ip dhcp snooping database write-delay` command to configure the interval in seconds at which the DHCP Snooping database will be stored in persistent storage. Use the “no” form of this command to reset the write delay to the default.

Syntax

```
ip dhcp snooping database write-delay seconds
no ip dhcp snooping database write-delay
```

- `seconds`—The write delay (Range: 15–86400 seconds).

Default Configuration
The write delay is 300 seconds by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example

```
console(config)#ip dhcp snooping database write-delay 500
```
ip dhcp snooping limit

Use the ip dhcp snooping limit command to diagnostically disable itself if the rate of received DHCP messages exceeds the configured limit. Use the no shutdown command to re-enable the interface. Use the no form of this command to disable automatic shutdown of the interface.

Syntax

ip dhcp snooping limit {rate rate [burst interval seconds]}
no ip dhcp snooping limit

- rate—The maximum number of packets per second allowed (Range: 0–300 pps).
- seconds—Interval over which to measure a burst of packets. (Range: 1–15 seconds).

Default Configuration

By default, DHCP messages do not cause an interface to be disabled.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command is available in Ethernet interface configuration mode or port channel interface configuration mode. The switch hardware rate limits DHCP packets sent to the CPU from snooping enabled interfaces to 512 Kbps.

To prevent DHCP packets from being used in a DoS attack when DHCP snooping is enabled; the snooping application allows configuration of rate limiting for received DHCP packets. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit within the configured interval, DHCP snooping shuts down the interface. The administrator must perform the “no shutdown” command on the affected interface to re-enable the interface.
The administrator can configure the rate and burst interval. Rate limiting is configured independently on each Ethernet or port-channel interface and may be enabled on both DHCP trusted and untrusted interfaces. The rate limit is configurable in the range of 0-300 packets per second and the burst interval in the range of 1-15 seconds. In general, a rate limit of under 100 pps is valid for untrusted interfaces.

Examples
console(config-if-Gi1/0/1)#ip dhcp snooping limit rate 100 burst interval 1

ip dhcp snooping log-invalid

Use the ip dhcp snooping log-invalid command to enable logging of DHCP messages filtered by the DHCP Snooping application. Use the no form of this command to disable logging.

Syntax
ip dhcp snooping log-invalid
no ip dhcp snooping log-invalid

Default Configuration
Logging of filtered messages is disabled by default.
Invalid DHCP messages are not logged by default.

Command Mode
Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines
This command is available in Ethernet interface configuration mode or port channel configuration mode.

Example
console(config-if-Gi1/0/1)#ip dhcp snooping log-invalid

console(config-if-Gi1/0/1)#no ip dhcp snooping log-invalid
**ip dhcp snooping trust**

Use the `ip dhcp snooping trust` command to configure a port as trusted. Use the `no` form of this command to configure a port as untrusted.

**Syntax**

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

**Default Configuration**

Ports are untrusted by default.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

Configuring an interface as trusted disables DHCP snooping validation of DHCP packets and exposes the port to IPv4 DHCP DoS attacks. Configuring an interface as untrusted indicates that the switch should firewall DHCP messages and act as if the port is connected to a device outside the DMZ.

DHCP snooping must be enabled globally and on the VLAN for which the port is a member for this command to have an effect.

Interfaces connected to the DHCP server must be configured as trusted in order for DHCP snooping to operate.

Use the `ip verify source` command to disallow traffic from untrusted sources on an interface.

**Example**

```
console(config-if-Gi1/0/1)#ip dhcp snooping trust
console(config-if-Gi1/0/1)#no ip dhcp snooping trust
```
ip dhcp snooping verify mac-address

Use the ip dhcp snooping verify mac-address command to enable the verification of the source MAC address with the client MAC address in the received DHCP message. Use the “no” form of this command to disable verification of the source MAC address.

Syntax
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Default Configuration
Source MAC address verification is disabled by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)#ip dhcp snooping verify mac-address

show ip dhcp snooping

Use the show ip dhcp snooping command to display the DHCP snooping global configuration.

Syntax
show ip dhcp snooping

Default Configuration
There is no default configuration for this command.
**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs: 11 - 30, 40

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Log Invalid Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**show ip dhcp snooping binding**
Use the `show ip dhcp snooping binding` command to display the DHCP snooping binding entries.

**Syntax**
```
show ip dhcp snooping binding [{static | dynamic}] [interface interface-id | port-channel port-channel-number] [vlan vlan-id]
```

- **static | dynamic**—Use these keywords to filter by static or dynamic bindings.
- **interface-id**—The Ethernet interface for which to show bindings.
- **port-channel-number**—The port channel for which to show bindings.
- **vlan-id**—The VLAN identifier for which to show bindings.
Default Configuration
There is no default configuration for this command.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show ip dhcp snooping binding

Total number of bindings: 2

+-----------------+------------+-----+---------+----+--------+
| MAC Address     | IP Address | VLAN| Interface| Type| Lease  |
+-----------------+------------+-----+---------+----+--------+
| 00:02:B3:06:60:80 | 210.1.1.3  | 10  | Gi1/0/1 | Dyn| 86400  |
| 00:02:FE:06:13:04 | 210.1.1.4  | 10  | Gi1/0/1 | Dyn| 86400  |

show ip dhcp snooping database

Use the show ip dhcp snooping database command to display the DHCP snooping configuration related to the database persistence.

Syntax
show ip dhcp snooping database

Default Configuration
There is no default configuration for this command.

Command Mode
User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.
Example
console#show ip dhcp snooping database

agent url: /10.131.13.79:/sail.txt

write-delay: 5000

show ip dhcp snooping interfaces

Use the show ip dhcp snooping interfaces command to show the DHCP Snooping status of the interfaces.

Syntax
show ip dhcp snooping interfaces [interface-id]
  • interface-id—A valid Ethernet or port-channel interface.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show ip dhcp snooping interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>

console#show ip dhcp snooping interfaces gigabitethernet 1/0/15

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
</table>
show ip dhcp snooping statistics

Use the `show ip dhcp snooping statistics` command to display the DHCP snooping filtration statistics.

**Syntax**

`show ip dhcp snooping statistics`

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed by this command:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Verify Failures</td>
<td>The number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client MAC address mismatch.</td>
</tr>
<tr>
<td>Client Ifc Mismatch</td>
<td>The number of DHCP release and Deny messages received on the different ports than previously learned.</td>
</tr>
<tr>
<td>DHCP Server Msgs Rec'd</td>
<td>The number of DHCP server messages received on untrusted ports.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ip dhcp snooping statistics

Interface     MAC Verify Failures     Client Ifc Mismatch   DHCP Server Msgs Rec'd
------------- --------------- --------------- ------------------ 
Gi1/0/2       0               0               0
Gi1/0/3       0               0               0
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>InOctets</th>
<th>InPkts</th>
<th>OutOctets</th>
<th>OutPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**DHCPv6 Snooping Commands**

**Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches**

This section explains the following commands:

- `clear ipv6 dhcp snooping binding`  
- `ipv6 dhcp snooping binding`  
- `ipv6 dhcp snooping`  
- `ipv6 dhcp snooping vlan`  
- `ipv6 dhcp snooping binding`  
- `ipv6 dhcp snooping database`  
- `ipv6 dhcp snooping database write-delay`  
- `ipv6 dhcp snooping limit`  
- `ipv6 dhcp snooping log-invalid`  
- `ipv6 dhcp snooping trust`  
- `ipv6 dhcp snooping verify mac-address`  
- `ipv6 verify binding`  
- `ipv6 verify source`  
- `show ipv6 dhcp snooping binding`  
- `show ipv6 dhcp snooping database`  
- `show ipv6 dhcp snooping interfaces`  
- `show ipv6 dhcp snooping statistics`  
- `show ipv6 source binding`  
- `show ipv6 verify`  
- `show ipv6 verify source`  

---

### clear ipv6 dhcp snooping binding

Use the `clear ipv6 dhcp snooping binding` command to clear all IPv6 DHCP Snooping entries.

**Syntax**

```
clear ipv6 dhcp snooping binding {* | interface interface-id}
```

- `*`—Clears all snooping bindings.
- `interface-id`—Clears all snooping bindings on a specified Ethernet interface.

**Default Configuration**

This command has no default configuration.
**Command Modes**
User Exec, Privileged Exec

**User Guidelines**
This command has no user guidelines.

**Example**
(console)#clear ipv6 dhcp snooping binding

**clear ipv6 dhcp snooping statistics**
Use the clear ipv6 dhcp snooping statistics command to clear all IPv6 DHCP Snooping statistics.

**Syntax**
clear ipv6 dhcp snooping statistics

**Default Configuration**
This command has no default configuration.

**Command Modes**
User Exec, Privileged Exec

**User Guidelines**
The IPv6 snooping statistics are also cleared by the clear counters command.

**Example**
(console)#clear ipv6 dhcp snooping statistics

**ipv6 dhcp snooping**
Use the ipv6 dhcp snooping command to globally enable IPv6 DHCP snooping. Use the no form of the command to globally disable IPv6 DHCP snooping.
Syntax
ipv6 dhcp snooping
no ipv6 dhcp snooping

Default Configuration
By default, DHCP snooping is not enabled.

Command Modes
Global Configuration mode

User Guidelines
The DHCP snooping application processes incoming DHCP messages. For RELEASE and DECLINE messages from a DHCPv6 client and RECONFIGURE messages from a DHCPv6 server received on an untrusted interface, the application compares the receive interface and VLAN with the client’s interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event and drops the packet. If configured, for valid client messages, DHCP snooping additionally compares the source MAC address to the DHCP client hardware address. If there is a mismatch, DHCP snooping logs a message and drops the packet. The network administrator can disable this option using the no ipv6 dhcp snooping verify mac-address for DHCPv6. DHCP snooping always forwards client messages on trusted interfaces within the VLAN. If DHCP relay or/and DHCP server are enabled simultaneously with DHCP snooping, the DHCP client message will be sent to the DHCP relay or/and DHCP server to process further.

Example
console(config)#ipv6 dhcp snooping

ipv6 dhcp snooping vlan
Use the ipv6 dhcp snooping vlan command to globally enable IPv6 DHCP on a set of VLANs. Use the no form of the command to globally disable IPv6 DHCP snooping on a set of VLANs.
**Syntax**

ipv6 dhcp snooping vlan vlan-list
no ipv6 dhcp snooping vlan-list

- **vlan-list** — A single VLAN, one or more VLANs separated by commas, or two VLANs separated by a single dash indicating all VLANs between the first and second inclusive. Multiple VLAN identifiers can be entered provided that no embedded spaces are contained within the vlan-list.

**Default Configuration**

By default, DHCP snooping is not enabled on any VLANs.

**Command Modes**

Global Configuration mode

**User Guidelines**

DHCP snooping must be enabled on at least one VLAN and globally enabled to become operational.

**Example**

```
console(config)#ipv6 dhcp snooping
console(config)#ipv6 dhcp snooping vlan 5-10,15,30
console(config)#interface Te1/0/1
console(config-if-Te1/0/1)#switchport mode access
console(config-if-Te1/0/1)#switchport access vlan 10
console(config-if-Te1/0/1)#no ipv6 dhcp snooping trust
```

**ipv6 dhcp snooping binding**

Use the `ipv6 dhcp snooping binding` command to configure a static IPv6 DHCP snooping binding. Use the `no` form of the command to remove the entry from the binding database.

**Syntax**

ipv6 dhcp snooping binding mac-address vlan vlan-id ip-address interface 
{gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port | port-channel port-channel-number}

no ipv6 dhcp snooping binding mac-address
• mac-address—A valid mac address in standard format.
• vlan-id — A configured VLAN id. (Range 1-4093)
• ip-address—A valid IPv6 address.
• interface-id—A valid Ethernet interface ID in short or long format.
• port-channel-number—A valid port channel identifier.

Default Configuration
By default, no static DHCP bindings are configured.

Command Modes
Global Configuration mode

User Guidelines
Static bindings do not age out of the DHCP binding database.

ipv6 dhcp snooping database
Use the ipv6 dhcp snooping database command to configure the persistent location of the DHCP snooping database. This can be a local or remote file on a TFTP server.

Syntax
ipv6 dhcp snooping database {local | tftp://hostIP/filename}
no ipv6 dhcp snooping database

Default Configuration
By default, the local database is used.

Command Modes
Global Configuration mode
**User Guidelines**

The DHCP binding database is persistently stored on a configured external server or locally in flash, depending on the user configuration. A row-wise checksum is placed in the text file that is stored on the configured TFTP server. On switch startup, the switch reads the text file and uses the contents to build the DHCP snooping database. If the calculated checksum value equals the stored checksum, the switch uses the entries from the binding file and populates the binding database. Checksum failure or a connection problem to the external configured server causes the switch to lose the bindings and may cause connectivity loss for hosts if IPSG or DAI is enabled.

**ipv6 dhcp snooping database write-delay**

Use the `ipv6 dhcp snooping database write-delay` command to configure the time period between successive writes of the binding database. The binding database is used to persistently store the DHCP bindings. Use the `no` form of the command to return the write delay to the default value.

**Syntax**

```
ipv6 dhcp snooping database write-delay seconds
no ipv6 dhcp snooping write-delay
```

- `seconds`—The period of time between successive writes of the binding database to persistent storage. (Range 15-86400 seconds.)

**Default Configuration**

By default, the write delay is 300 seconds.

**Command Modes**

Global Configuration mode

**User Guidelines**

The binding database is cached in memory and written to storage every write-delay seconds.
**ipv6 dhcp snooping limit**

Use the `ipv6 dhcp snooping limit` command configures an interface to be diagnostically disabled if the rate of received DHCP messages exceeds the configured limit. Use the `no shutdown` command to reenable the interface. Use the no form of the command to disable diagnostic disabling of the interface.

**Syntax**

`ipv6 dhcp snooping limit {rate pps [burst interval seconds]}
no ipv6 dhcp snooping limit`

- **pps**—The rate in packets per interval. (Range 0-300.)
- **seconds**—The time interval over which to measure a burst of packets. (Range 1-15, default 1 second.)

**Default Configuration**

By default, DHCP messages do not shut down the interface.

**Command Modes**

Interface Configuration mode

**User Guidelines**

The switch hardware rate limits DHCP packets sent to the CPU from snooping enabled interfaces to 512 Kbps.

To prevent DHCP packets from being used in a DoS attack when DHCP snooping is enabled, the snooping application allows configuration of rate limiting for received DHCP packets. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit within the configured interval, DHCP snooping diagnostically disables the interface. The administrator must perform the `no shutdown` command on the affected interface to reenable the interface.
The administrator can configure the rate and burst interval. Rate limiting is configured independently on each Ethernet interface and may be enabled on both trusted and untrusted interfaces. The rate limit is configurable in the range of 0-300 packets per second and the burst interval in the range of 1-15 seconds.

**ipv6 dhcp snooping log-invalid**

Use the `ipv6 dhcp snooping log-invalid` command to configure the port to log invalid received DHCP messages.

**Syntax**

```
ipv6 dhcp snooping log-invalid
no ipv6 dhcp snooping log-invalid
```

**Default Configuration**

By default, invalid DHCP messages are not logged.

**Command Modes**

Interface Configuration mode

**User Guidelines**

An invalid DHCP message is one that is received on an untrusted interface that is not a member of the VLAN over which the IP address (and optionally the MAC address) has been learned. Receiving large number of invalid messages may be an indication of an attack.

Logging invalid messages can use valuable CPU resources if the switch receives such messages at a high rate. To avoid allowing the switch to be vulnerable to a DoS attack, DHCP snooping only logs invalid messages if the user has enabled logging. Logging is enabled on individual interfaces so that only messages on interfaces of interest are logged. To further protect the system, invalid message logging is rate limited to 1 per second.
ipv6 dhcp snooping trust

Use the ipv6 dhcp snooping trust command to configure an interface as trusted. Use the no form of the command to return the interface to the default configuration.

Syntax

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Default Configuration

By default, interfaces are untrusted.

Command Modes

Interface Configuration mode (Ethernet and port-channel)

User Guidelines

Configuring an interface as trusted disables DHCP snooping address validation checking and exposes the port to IPv6 DHCP DoS attacks.

DHCP snooping must be enabled globally and on the VLAN for which the port is a member for this command to have an effect. Configuring a port as trusted indicates that the port is connected to an IPv6 DHCP server or to a trusted device. Configuring a port as untrusted indicates that the switch should firewall IPv6 DHCP messages and act as if the port is connected to an untrusted device.

Use the ipv6 verify source command to disable traffic from untrusted sources on an interface.

ipv6 dhcp snooping verify mac-address

Use the ipv6 dhcp snooping verify mac-address command to enable the additional verification of the source MAC address with the client hardware address in the received DHCP message.

Syntax

ipv6 dhcp snooping verify mac-address
no ipv6 dhcp snooping verify mac-address

**Default Configuration**
By default, MAC address verification is not enabled.

**Command Modes**
Global Configuration mode

**User Guidelines**
DHCP MAC address verification operates on DHCP messages received over untrusted interfaces. The source MAC address of DHCP packet is different from the client hardware if:

- A DHCP discovery/request broadcast packet that was forwarded by the relay agent.
- A DHCP unicast request packet was routed in renew process.

For DHCP servers and relay agents connected to untrusted interfaces, source MAC verification should be disabled.

DHCP snooping must be enabled on at least one VLAN and globally enabled to become operational.

**Example**
```bash
console(config)#ipv6 dhcp snooping
console(config)#ipv6 dhcp snooping vlan 5-10,15,30
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport mode access
console(config-if-Te1/0/1)#switchport access vlan 10
console(config-if-Te1/0/1)#no ipv6 dhcp snooping trust
console(config-if-Te1/0/1)#exit
console(config)#ipv6 dhcp snooping verify mac-address
```

**ipv6 verify binding**

Use the `ipv6 verify binding` command to configure a static IP source guard binding.
Syntax

ipv6 verify binding mac-address vlan vlan-id ip-address interface interface id
no ipv6 verify binding mac-address vlan vlan-id ip-address interface interface id

- mac-address — A valid mac address in standard format.
- vlan-id — A configured VLAN id. (Range 1-4093.
- ip-address — A valid IPv6 address.
- interface-id—A valid interface ID in short or long format.

Default Configuration

By default, no static IP Source Guard entries are configured.

Command Modes

Global Configuration mode

User Guidelines

Traffic is filtered based upon the source IPv6 address and VLAN. Use the switchport port-security command in interface mode to optionally add MAC address filtering in addition to source IPv6 address filtering. If port security is enabled, the filtering is based upon IPv6 address, MAC address and VLAN.

ipv6 verify source

Use the ipv6 verify source command to configure an interface to filter (drop) incoming traffic from sources that are not present in the DHCP binding database. Use the no form of the command to enable unverified traffic to flow over the interfaces.

Syntax

ipv6 verify source [port-security]
no ipv6 verify source

- port-security — Enables filtering based upon source IP address, VLAN and MAC address.
Default Configuration
By default, no sources are blocked.

Command Modes
Interface Configuration mode (Ethernet and port-channel)

User Guidelines
DHCP snooping should be enabled on any interfaces for which ipv6 verify source is configured. If ipv6 verify source is configured on an interface for which DHCP snooping is disabled, or for which DHCP snooping is enabled and the interface is trusted, incoming traffic on the interface is dropped.

Traffic is filtered based on the source IP address and VLAN. When the port-security keyword is configured, filtering occur based upon source IP address, VLAN and source MAC address.

IP source guard also interacts with the port security component. Use the port security command in interface mode to optionally add checking of learned MAC addresses. When port security is enabled, MAC learning coordinates with the IP Source Guard component to verify that the MAC address is in the DHCP binding database. If it is not, port security is notified that the frame is in violation of the security policy.

show ipv6 dhcp snooping
Use the show ipv6 dhcp snooping command to display the IPv6 DHCP snooping configuration

Syntax
show ipv6 dhcp snooping

Default Configuration
This command has no default configuration.

Command Modes
User Exec, Privileged Exec (all show modes)
User Guidelines
This command has no user guidelines.

Example
(console)#show ipv6 dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs: 11 - 30, 40

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Log Invalid Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

show ipv6 dhcp snooping binding
Use the show ipv6 dhcp snooping binding command to display the IPv6 DHCP snooping configuration

Syntax
show ipv6 dhcp snooping binding [{static|dynamic}] [interface interface-id | port-channel port-channel-number] [vlan vlan-id]

- static—Only show static entries.
- dynamic—Only show dynamic entries.
- interface-id—Limit the display to entries associated with Ethernet interface-id.
- vlan-id—Limit the display to entries associated with VLAN vlan-id.
- port-channel-number—Limit the display to entries associated with the identified port channel.

Default Configuration
This command has no default configuration.
Command Modes
User Exec, Privileged Exec (all show modes)

User Guidelines
There are no user guidelines for this command.

Example
(console)#show ipv6 dhcp snooping binding

Total number of bindings: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IPv6 Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Lease time(Secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:06:60:80</td>
<td>2000::1/64</td>
<td>10</td>
<td>0/1</td>
<td>86400</td>
</tr>
<tr>
<td>00:0F:FE:00:13:04</td>
<td>3000::1/64</td>
<td>10</td>
<td>0/1</td>
<td>86400</td>
</tr>
</tbody>
</table>

show ipv6 dhcp snooping database

Use the show ipv6 dhcp snooping database command to display IPv6 DHCP snooping configuration related to database persistency.

Syntax
show ipv6 dhcp snooping database

Default Configuration
This command has no default configuration.

Command Modes
User Exec, Privileged Exec (all show modes)

User Guidelines
This command has no user guidelines.

Example
(console)#show ipv6 dhcp snooping database

agent url: /10.131.13.79:/sail.txt
show ipv6 dhcp snooping interfaces

Use the show ipv6 dhcp snooping interfaces command to show the DHCP Snooping status of IPv6 interfaces.

Syntax

show ipv6 dhcp snooping interfaces [interface id]
  •  interface id—A valid Ethernet or port-channel interface.

Default Configuration

There is no default configuration for this command.

Command Modes

User Exec, Privileged Exec (all show modes)

User Guidelines

If no parameter is given, all interfaces are shown.

Example

(console)#show ipv6 dhcp interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>

show ipv6 dhcp snooping statistics

Use the show ipv6 dhcp snooping statistics command to display IPv6 dhcp snooping filtration statistics.
Syntax
show ipv6 dhcp snooping statistics

Default Configuration
This command has no default configuration.

Command Modes
User Exec, Privileged Exec (all show modes)

User Guidelines
The following statistics are displayed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Verify Failures</td>
<td>The number of DHCP messages that got filtered on an untrusted interface because of the source MAC address and client hardware address mismatch.</td>
</tr>
<tr>
<td>Client Ifc mismatch</td>
<td>The number of DHCP release and reply messages received on different ports than the ones they were learned on previously.</td>
</tr>
<tr>
<td>DHCP Server Msgs</td>
<td>It represents the number of DHCP server messages received on Untrusted ports.</td>
</tr>
</tbody>
</table>

Example
(console)#show ipv6 dhcp snooping statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Verify Failures</th>
<th>Client Ifc Mismatch</th>
<th>DHCP Server Msgs Rec'd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show ipv6 source binding

Use the show ipv6 source binding command to display the IPv6 Source Guard configurations on all ports, on an individual port, or on a VLAN.

Syntax

show ipv6 source binding [{dhcp-snooping | static}] [interface interface-id] [vlan vlan-id]

- dhcp-snooping — Displays the DHCP snooping bindings.
- static — Displays the statically configured bindings.

Default Configuration

This command has no default configuration.

Command Modes

User Exec, Privileged Exec (all show modes)

User Guidelines

This command has no user guidelines.

Example

(console)#show ipv6 source binding

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Type</th>
<th>Vlan</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:08</td>
<td>2000::1</td>
<td>dhcpv6-snooping</td>
<td>2</td>
<td>Gi1/0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:09</td>
<td>3000::1</td>
<td>dhcpv6-snooping</td>
<td>3</td>
<td>Gi1/0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:0A</td>
<td>4000::1</td>
<td>dhcpv6-snooping</td>
<td>4</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

show ipv6 verify

Use the show ipv6 verify command to display the IPv6 Source Guard configuration on all interfaces or the specified interface.

Syntax

show ipv6 verify [interface if-id]

- if-id — A valid interface ID (Ethernet)
Default Configuration
There is no default configuration for this command.

Command Modes
User Exec, Privileged Exec (all show modes)

User Guidelines
The filter type is one of the following values:

- ipv6-mac: User has configure MAC address filtering on this interface
- ipv6: IPv6 address filtering is configured on this interface
- N/A: No filtering is configured on the interface

Example

console(config-if-Gi1/0/5)#show ipv6 verify

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>ipv6</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>ipv6-mac</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>ipv6-mac</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>N/A</td>
</tr>
</tbody>
</table>

console(config-if-Gi1/0/5)#show ipv6 verify interface gi1/0/5

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/5</td>
<td>ipv6-mac</td>
</tr>
</tbody>
</table>

show ipv6 verify source

Use the show ipv6 verify source command to display the IPv6 Source Guard configurations on all ports.
**Syntax**

```
show ipv6 verify source
```

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

User Exec, Privileged Exec (all show modes)

**User Guidelines**

If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, the MAC Address field displays permit-all.

The filter type is one of the following:

- `ipv6-mac`: User has configured MAC address filtering on this interface.
- `ipv6`: Only IPv6 address filtering is configured on this interface.

**Example**

```
show ipv6 verify source
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
<th>IPv6 Address</th>
<th>MAC Address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>ipv6-mac</td>
<td>2000::1/64</td>
<td>00:02:B3:06:60:80</td>
<td>10</td>
</tr>
<tr>
<td>Gi1/0/1</td>
<td>ipv6-mac</td>
<td>3000::1/64</td>
<td>00:0F:FE:00:13:04</td>
<td>10</td>
</tr>
</tbody>
</table>
Dynamic ARP Inspection Commands

Dell EMC Networking N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its neighbors. The attacker sends ARP requests or responses mapping another station IP address to its own MAC address. DAI drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP Snooping bindings database.

Commands in this Section

This section explains the following commands:

```plaintext
arp ip access-list
clear ip arp inspection statistics
ip arp inspection filter
ip arp inspection limit
ip arp inspection trust
ip arp inspection validate
ip arp inspection vlan
permit ip host mac host
show arp access-list
show ip arp inspection
12 Enabled Disabled
```

arp ip access-list

Use the `arp access-list` command to create an ARP ACL. It will place the user in ARP ACL Configuration mode. Use the “no” form of this command to delete an ARP ACL.

**Syntax**

`arp ip access-list acl-name`

`no arp ip access-list acl-name`
• acl-name — A valid ARP ACL name (Range: 1–31 characters).

**Default Configuration**
There are no ARP ACLs created by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config)#arp access-list tier1
```

**clear ip arp inspection statistics**

Use the `clear ip arp inspection statistics` command to reset the statistics for Dynamic Address Resolution Protocol (ARP) inspection on all VLANs.

**Syntax**
clear ip arp inspection statistics

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#clear ip arp inspection statistics
```
**ip arp inspection filter**

Use the `ip arp inspection filter` command to configure an ARP ACL to be used for a single VLAN or a range of VLANs to filter invalid ARP packets. Use the “no” form of this command to remove the ARP ACL.

**Syntax**

```
ip arp inspection filter acl-name vlan vlan-list [static]
no ip arp inspection filter acl-name vlan vlan-list [static]
```

- `acl-name` — The name of a valid ARP ACL. (Range: 1–31 characters)
- `vlan-list` — A list of VLAN identifiers. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

**Default Configuration**

No ARP ACL is configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

**Example**

```
console(config)#ip arp inspection filter tier1 vlan 2-10 static
console(config)#ip arp inspection filter tier1 vlan 20-30
```

**ip arp inspection limit**

Use the `ip arp inspection limit` command to configure the rate limit and burst interval values for an interface.

Configuring `none` for the limit means the interface is not rate limited for Dynamic ARP Inspection.
Syntax

ip arp inspection limit {none | rate pps [burst interval seconds]}
no ip arp inspection limit

- none — To set no rate limit.
- pps — The number of packets per second (Range: 0–300).
- seconds — The number of seconds (Range: 1–15).

Default Configuration

The default rate limit is 15 packets per second.
The default burst interval is 1 second.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

If Dynamic ARP Inspection packets are received on a port at a rate that exceeds the threshold for a specified time, that port will be diagnostically disabled. The threshold is configurable up to 300 pps, and the burst is configurable up to 15s long. The default is 15 pps and 1s burst.

Use the no shut command to bring the port back in to service.

Example

console(config-if-Gi1/0/1)#ip arp inspection limit none
console(config-if-Gi1/0/1)#ip arp inspection limit rate 100 burst interval 2

ip arp inspection trust

The ip arp inspection trust command configures an interface as trusted for Dynamic ARP Inspection. Use the no form of this command to configure an interface as untrusted.

Syntax

ip arp inspection trust
no ip arp inspection trust
Default Configuration
Interfaces are configured as untrusted by default.

Command Mode
Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines
ARP responses received on a trusted interface are not checked against the DHCP snooping bindings. They are entered into the ARP cache without filtering.

Example
console(config-if-Gi1/0/3)#ip arp inspection trust

ip arp inspection validate
Use the `ip arp inspection validate` command to enable additional validation checks on received ARP packets.

Syntax
```
ip arp inspection validate {[src-mac] [dst-mac] [ip]}
no ip arp inspection validate {[src-mac] [dst-mac] [ip]}
```
- **src-mac**—For validating the source MAC address of an ARP packet.
- **dst-mac**—For validating the destination MAC address of an ARP packet.
- **ip**—For validating the IP address of an ARP packet.

Default Configuration
There is no additional validation enabled by default.

Command Mode
Global Configuration mode
**User Guidelines**

By default Dynamic ARP Inspection validates the source MAC address and source IP address in received ARP responses against the DHCP Snooping bindings. ARP responses that fail the check are discarded without updating the ARP cache. This command enables additional validation checks on ARP response packets before updating the ARP cache. Any combination of checks is allowed.

Each command invocation overrides the current configuration. For example, if the existing configuration enables source MAC address and destination MAC address validation and a command is issued to enable IP address validation only, the source MAC address and destination MAC address validations are disabled and IP address validation is enabled. Use the **no** form of this command to disable all additional validation checks.

**Example**

```
console(config)#ip arp inspection validate src-mac dst-mac ip
console(config)#ip arp inspection validate src-mac ip
console(config)#ip arp inspection validate dst-mac ip
console(config)#ip arp inspection validate ip
```

**ip arp inspection vlan**

Use the **ip arp inspection vlan** command to enable Dynamic ARP Inspection on a single VLAN or a range of VLANs. Use the **no** form of this command to disable Dynamic ARP Inspection on a single VLAN or a range of VLANs.

**Syntax**

```
ip arp inspection vlan vlan-list [logging]
no ip arp inspection vlan vlan-list [logging]
```

-   **vlan-list** — A list of VLAN identifiers. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)
-   **logging** — Use this parameter to enable logging of invalid packets.

**Default Configuration**

Dynamic ARP Inspection is disabled by default.
**Command Mode**
Global Configuration mode

**User Guidelines**
Dynamic ARP Inspection validates the source MAC address and source IP address in received ARP responses against the DHCP Snooping bindings. ARP responses that fail the check are discarded without updating the ARP cache.

**Example**
```
console(config)#ip arp inspection vlan 200-300
console(config)#ip arp inspection vlan 200-300 logging
```

**permit ip host mac host**
Use the `permit ip host mac host` command to configure an IP address and MAC address combination used in ARP packet validation. Use the “no” form of this command to delete the ARP ACL rule.

**Syntax**
```
permit ip host sender-ip mac host sender-mac
no permit ip host sender-ip mac host sender-mac
```
- `sender-ip` — Valid IP address used by a host.
- `sender-mac` — Valid MAC address in combination with the above `sender-ip` used by a host.

**Default Configuration**
There are no ARP ACL rules created by default.

**Command Mode**
ARP Access-list Configuration mode

**User Guidelines**
There are no user guidelines for this command.
Example

console(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05

**show arp access-list**

Use the `show arp access-list` command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument would display only the rules in that ARP ACL.

**Syntax**

`show arp access-list [acl-name]`

- acl-name — A valid ARP ACL name (Range: 1–31 characters).

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

console#show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07

ARP access list H3

ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08

**show ip arp inspection**

Use the `show ip arp inspection` command to display the Dynamic ARP Inspection and status.
Syntax

show ip arp inspection [interfaces [interface-id] | statistics [vlan vlan-list] | vlan vlan-list]

- **interfaces [interface-id]**—Display the Dynamic ARP Inspection configuration on all the DAI enabled interfaces. Giving an interface argument, it displays the values for that interface only.
- **statistics [vlan vlan-list]**—Display the statistics of the ARP packets processed by Dynamic ARP Inspection. Given vlan-list argument, it displays the statistics on all DAI-enabled VLANs in that range. In the case of no argument, it lists the summary of the forwarded and dropped ARP packets.
- **vlan vlan-list**—Display the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN list. It also displays the global configuration values for source MAC validation, destination MAC validation and invalid IP validation. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following information is displayed for each VLAN when a VLAN range is supplied:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The VLAN-ID for each displayed row.</td>
</tr>
<tr>
<td>DHCP Drops</td>
<td>The number of packets dropped due to DHCP Snooping binding database match failure.</td>
</tr>
<tr>
<td>ACL Drops</td>
<td>The number of packets dropped due to ARP ACL rule match failure.</td>
</tr>
</tbody>
</table>
Layer 2 Switching Commands

### Example

Following is an example of the `show ip arp inspection` command.

```markdown
console#show ip arp inspection

Source MAC Validation................. Disabled
Destination MAC Validation............ Disabled
IP Address Validation................. Disabled

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Configuration Log Invalid</th>
<th>ACL Name</th>
<th>Static flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>
```

Following is an example of the `show ip arp inspection interfaces` command.

```markdown
console#show ip arp inspection interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Untrusted</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Untrusted</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>
```

Following is an example of the `show ip arp inspection statistics` command.

```markdown
console#show ip arp inspection statistics

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>90</td>
<td>14</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td>3</td>
</tr>
</tbody>
</table>
```

```markdown
console#show ip arp inspection statistics vlan 10,20
```
<table>
<thead>
<tr>
<th>VLAN</th>
<th>DHCP Drops</th>
<th>ACL Permits</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Bad Src MAC</th>
<th>Bad Dest MAC</th>
<th>Invalid IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>11</td>
<td>1</td>
<td>65</td>
<td>25</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The following global parameters are displayed when no parameters are given:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Mac Validation</td>
<td>If Source Mac validation of ARP frame is enabled.</td>
</tr>
<tr>
<td>Destination Mac Validation</td>
<td>If Destination Mac validation of ARP Response frame is enabled.</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>If IP address validation of ARP frame is enabled.</td>
</tr>
</tbody>
</table>

The following fields are displayed for each VLAN:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The VLAN-ID for each displayed row.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Whether DAI is enabled on the VLAN.</td>
</tr>
<tr>
<td>Log Invalid</td>
<td>Whether logging of invalid ARP packets is enabled on the VLAN.</td>
</tr>
<tr>
<td>ACL Name</td>
<td>ARP ACL Name if configured on the VLAN.</td>
</tr>
<tr>
<td>Static flag</td>
<td>If the ARP ACL is configured static on the VLAN.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ip arp inspection vlan 10-12
```

**Source Mac Validation**: Disabled
**Destination Mac Validation**: Disabled
**IP Address Validation**: Disabled

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>Log Invalid</th>
<th>ACL Name</th>
<th>Static flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enabled</td>
<td>Enabled</td>
<td>H2</td>
<td>Enabled</td>
</tr>
<tr>
<td>11</td>
<td>Disabled</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ethernet Configuration Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dell EMC Networking switches support a variety of configuration options to optimize network operations. Features such as flow-control and jumbo frames are supported along with a variety of commands to display traffic statistics as well as limit the effects of network loops or other network issues.

Jumbo frame technology is employed in certain situations to reduce the task load on a server CPU and to transmit large amounts of data efficiently. Jumbo frames technology predominantly appears where certain applications would benefit from using a larger frame size, e.g. Network File System (NFS). The larger frame size eliminates some of the need for fragmentation, leading to greater throughput. The increase in throughput is particularly valuable on data center servers where the larger frame size increases efficiency of the system and allows processing of more requests. The Dell EMC Networking jumbo frames feature extends the standard Ethernet MTU (Max Frame Size) from 1518 (1522 with VLAN header) bytes to 9216 bytes. However, any device connecting to the same broadcast domain should support the same or larger MTU.

Flow control is a mechanism or protocol used to temporarily suspend transmission of data to a device to avoid overloading the device receive path. Dell EMC Networking switching implements the flow control mechanism defined in IEEE 802.3 Annexes 31A and 31B (formerly IEEE 802.3x). Dell EMC Networking switches implement receive flow control only. They never issue a flow control PAUSE frame when congested, but do respect flow control PAUSE frames received from other switches. Disabling flow control causes the switch to ignore received PAUSE frames. Flow control is enabled by default for all ports.

Storm control allows for rate limiting of specific types of packets through the forwarding plane. The administrator can configure the absolute rate in packets-per-second for the Storm control threshold. Each classified packet type (broadcast, multicast, or unicast) can be enabled/disabled per port, and the threshold level at which Storm-Control is active is also configurable per-port and per-type (as a percentage of interface speed).
On a storm control enabled interface, if the ingress rate of that type of packet (L2 broadcast, multicast, or unicast) is greater than the configured threshold level (as a percentage of port speed or as an absolute packets-per-second rate), the switch forwarding-plane discards the excess traffic.

The `speed` command controls interface link speeds and auto-negotiation. If speed is set to something other than auto, auto-negotiation is disabled on the interface. Auto-negotiation will link at the highest possible speed supported on the interface at full duplex.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear counters</th>
<th>show interfaces configuration</th>
<th>show storm-control</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>show interfaces counters</td>
<td>show storm-control action</td>
</tr>
<tr>
<td>default (interface)</td>
<td>show interfaces debounce</td>
<td>shutdown</td>
</tr>
<tr>
<td>duplex</td>
<td>show interfaces description</td>
<td>speed</td>
</tr>
<tr>
<td>flowcontrol</td>
<td>show interfaces detail</td>
<td>switchport protected</td>
</tr>
<tr>
<td>interface</td>
<td>show interfaces status</td>
<td>switchport protected name</td>
</tr>
<tr>
<td>interface range</td>
<td>show interfaces transceiver</td>
<td>show switchport protected</td>
</tr>
<tr>
<td>link debounce time</td>
<td>show interfaces trunk</td>
<td>show system mtu</td>
</tr>
<tr>
<td>rate-limit cpu</td>
<td>show statistics</td>
<td>system jumbo mtu</td>
</tr>
<tr>
<td>show interfaces</td>
<td>show statistics switchport</td>
<td>–</td>
</tr>
<tr>
<td>show interfaces advertise</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

**clear counters**

Use the `clear counters` command to clear statistics on an interface.

**Syntax**

`clear counters [vrf vrf-name | stack-ports | switchport | interface-id]`

- `vrf-name`—The name of the VRF instance on which the command operates.
• stack-ports—Clears stack-port statistics.
• switchport—Clear all the interface counters
• interface-id—An Ethernet or port-channel identifier. If specified, counters are cleared for the individual interface.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
Use of the clear counters command with no parameters indicates that both switch and all interface statistics are to be cleared. This command clears the individual component counters. If a port-channel is specified, the command clears the port channel counters, including the flap counters.
The VRF identified in the parameter must have been previously created or an error is returned.

Example
In the following example, the counters for port Gi1/0/1 are cleared.

console#clear counters gigabitethernet 1/0/1

description
Use the description command in Interface Configuration mode to add a description to an interface. To remove the description use the no form of this command.

Syntax
description string
no description

• string — Comment or a description of the port attached to this interface. (Range: 1 to 64 characters)
**Default Configuration**

By default, the interface does not have a description.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example adds a description to the Ethernet port 5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)# description RD_SW#3
```

**default (interface)**

Use the default interface command to configure the interface to the defaults.

**Syntax**

default [interface-id]

- interface-id—An Ethernet or port channel, loopback, tunnel or VLAN interface identifier.

**Default Configuration**

This command has no defaults.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command returns an Ethernet, port channel, VLAN, tunnel or loopback interface to the interface defaults as follows:

- Trunk and general mode configuration is removed.
• The interface is set to access mode using VLAN 1.
• The port is removed from all access-groups.
• The port is removed from port-channels.
• Speed/duplex are set to defaults.
• Spanning tree is enabled.
• Loop protection, BFD, and UDLD are disabled.
• Port MAC locking is disabled.
• Static MAC address entries referencing the interface are removed.
• Private VLAN configuration is removed.

Use of this command may cause the interface to drop the link. This is particularly true when the port defaults to a 10G fiber port and the installed transceiver requires auto-negotiation to be enabled.

**Command History**
Command introduced in version 6.5 firmware.

**Example**
```
console(config)#default gi1/0/1
```

**duplex**

Use the `duplex` command in Interface Configuration mode to configure the duplex operation of a given Ethernet interface. To restore the default, use the `no` form of this command.

**Syntax**
duplex {auto | half | full}

no duplex

• **auto**—Enable auto-negotiation for the port.
• **half**—Force half-duplex operation and disable auto-negotiation.
• **full**—Force full-duplex operation and disable auto-negotiation.
**Default Configuration**

Auto-negotiation is enabled by default on copper ports.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

When both speed and duplex are configured to auto, auto negotiation is enabled for the port. To disable auto-negotiation on a port, it is necessary to enter either the speed or duplex commands without using the auto parameter. 10G/40G fiber ports do not support auto-negotiation and therefore require the operator to enter the duplex full command and the speed command with the desired operating bandwidth. Auto-negotiation is required on 1G/10G/40G copper ports and 1G fiber ports.

The duplex command is only available on the Dell EMC Networking N1500 Series switches. Other switch models support full duplex operation only.

**Example**

The following example configures the duplex operation of TenGigabit Ethernet port Te 1/0/5 to force full duplex operation, disable auto-negotiation, and set the speed to 1000M.

```
console(config)# interface te1/0/5
console(config-if-Te1/0/5)# duplex full
console(config-if-Te1/0/5)# speed 1000
```

**flowcontrol**

Use the `flowcontrol` command in Global Configuration mode to configure the flow control. To disable flow control, use the `no` form of this command.

**Syntax**

```
flowcontrol receive {on | off}
no flowcontrol receive
```

**Default Configuration**

Flow Control is enabled by default.
**Command Mode**
Global Configuration and Interface Configuration modes

**User Guidelines**
Dell EMC Networking switches implement receive flow control only. They never issue a flow control PAUSE frame when congested, but do respect received flow control PAUSE frames received from other switches. Disabling flow control causes the switch to ignore received PAUSE frames.

Interface specific configuration overrides any global configuration.

Changing the flow control setting on a copper port restarts auto-negotiation and causes a brief link-flap while auto-negotiation occurs. Changing the flow control setting on a fiber port may cause a brief link flap as the PHY is reset.

Enabling flow control on some ports and not others can lead to excessive packet loss in situations where some ports on the switch have been paused and the internal packet buffers are consumed. This situation may cause traffic loss on other ports that are not congested or flow controlled.

**Example**
```
console(config)#flowcontrol receive off
console(config)#flowcontrol receive on
```

**interface**

Use this command to configure parameters for the Gigabit Ethernet and ten-Gigabit Ethernet ports, and for port-channels. While in Global Configuration mode, enter the **interface** command (with a specific interface). To exit to Global Configuration mode, enter `exit`. To return to Privileged Exec mode, press Ctrl-Z or enter `end`.

Additional forms of the interface command enable configuring VLANs, tunnels, the loopback interface, the out-of-band interface, and ranges of interfaces. See `interface vlan`, `interface tunnel`, `arp`, and `interface range`.

**Syntax**
```
interface { gigabitethernet unit/slot/port | port-channel port-channel-number |
            tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port }
```
**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration, Interface Configuration

**User Guidelines**
Dell EMC Networking switches implement receive flow control only. They never issue a flow control PAUSE frame when congested, but will respect received flow control PAUSE frames received from other switches. Disabling flow control causes the switch to ignore received PAUSE frames.

Interface specific configuration overrides any global configuration.

Changing the flow control setting on a copper port will restart auto-negotiation and cause a brief link-flap while auto-negotiation occurs.

Changing the flow control setting on a fiber port may cause a brief link flap as the PHY is reset.

Enabling flow control on some ports and not others can lead to excessive packet loss in situations where some ports on the switch have been paused and the internal packet buffers are consumed. This situation may cause traffic loss on other ports that are not congested or flow controlled. See [http://www.ieee802.org/3/cm_study/public/september04/thaler_3_0904.pdf](http://www.ieee802.org/3/cm_study/public/september04/thaler_3_0904.pdf) for more information.

**Example**
The following example enables Gigabit port 2 on stack member 1 for configuration.

```
console(config)# interface gigabitethernet 1/0/2
```

**interface range**
Use the `interface range` command in Global Configuration mode to execute a command on multiple ports at the same time.

- **NOTE:** An additional form of this command enables configuring a range of VLANs. See `interface range vlan`. 

Syntax

interface range {interface-range-specifier | interface-type all}

- port-range—A list of valid ports to configure. Separate non-consecutive ports with a comma and no spaces; use a hyphen to designate a range of ports. For more detailed information, see Command line parameters are entered by the user to choose an individual value or range of values for the specific command. Command line parameters are not syntax or range checked until the carriage return is entered. In some cases, the user may need to enter special characters, most often in a string parameter such as a password or a label. Special characters are one of the following characters (\"! $ % ^ & * ( ) _ - + = { } ] : ; @ ' " ~ # | \ < , > ./) or a blank. In these cases, it may be necessary to enclose the entire string in double or single quotes for the command line parser to properly interpret the parameter. The command line buffer parses up to the maximum number of command line characters possible in the port-range parameter.

- port-type—Shows all interfaces of the specified type.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration, Interface Range and Interface modes

User Guidelines

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

If a range of interfaces is specified using the dash notation, the beginning range number (to the left of the hyphen) must be less than or equal to the last number (to the right of the hyphen).
Example
The following example shows how gigabitethernet ports 5/0/18 to 5/0/20 and 3/0/1 to 3/0/24 are ranged to receive the same command.

console(config)# interface range gigabitethernet 5/0/18-20,Gi3/0/1-24
console(config-if-range)#

The following example shows how all gigabitethernet ports can be configured at once.

console(config)# interface range gigabitethernet all
console(config-if-range)#

The following examples demonstrate various valid interface ranges:

console(config)#interface range gigabitEthernet 1/0/1-20
console(config)#interface range gi1/0/20-48
console(config)#interface range gi1/0/1,gi1/0/48
console(config)#interface range gi2/0/1-10,gi1/0/30
console(config)#interface range gi1/0/1-10,gi1/0/30-48
console(config)#interface range gi1/0/1,te1/1/1
console(config)#interface range gigabitEthernet 1/0/10,te1/1/2

link debounce time
Use the `link debounce time` command to configure the debounce timer for one or multiple interfaces. Use the `no` form of the command to set the link debounce time to the default (disabled).

Syntax

link debounce time [ timeout ]

no link debounce time

- timeout—An integer value in the range of 100–5000 milliseconds. The timeout value must be a multiple of 100.

Default Configuration
Ethernet interfaces do not have debounce enabled by default.

Command Mode
Interface (Ethernet) Configuration mode, Interface Range mode.
User Guidelines

The link bounce time configures a link bounce hysteresis on link loss of link. Loss of link signal starts a link bounce timer. If the link is restored prior to expiry of the timer, operation continues and the system is not notified that that link connectivity has been lost. Hysteresis can be used to mitigate link flaps caused by bad cabling or partially inserted optics or cables.

The debounce timer resolution is approximately 10 ms. Setting a value will start the timer when loss of link is detected.

Ports operating at lower speeds may benefit from debounce values larger than the default. Ports operating over fiber generally do not require larger debounce times.

Use the show interfaces debounce command to display the link debounce time or to display the link flap count (the number of notifications sent to the system that link signal was lost). The link flap count is also displayed by the show interfaces command (Link Debounce Flaps).

The link debounce counter is cleared by the clear counters command and the clear counters interface-id command.

In general, a debounce time above 300 ms is recommended for copper interfaces with link flaps.

Command History

Introduced in version 6.2.0.1 firmware.

Example

The following example disables the link debounce timer for interface gi1/0/1.

```
switch# conf t
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#no link debounce time
```

The following example sets the link debounce timer for interface gi1/0/1 to 500 ms.

```
switch# conf t
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#link debounce time 500
```
**rate-limit cpu**

Use the *rate-limit cpu* command to reduce the amount of unknown unicast/multicast packets forwarded to the CPU. Use the *no* form of the command to set the rate limit to the default value.

**Syntax**

```
rate-limit cpu direction input pps pps_value
no rate-limit cpu direction input pps
```

- pps_value—The packets per second. The range is 100-1024 packets per second (100-3000 packets per second for N4000 series switches).

**Default Configuration**

The default ingress rate limit is 1024 packets per second (3000 for N4000 series switches).

**Command Modes**

Global Configuration mode

**User Guidelines**

Unknown unicast and multicast packets are copied to the CPU on the lowest priority QoS queue. Unknown packets are those that do not have hardware forwarding entries. Known unicast/multicast packets are hardware forwarded and are not queued to the CPU. Control plane packets (e.g. spanning tree BPDUs) are copied or forwarded to the CPU on higher priority queues. The rate limiting for unknown packets occurs on the internal CPU port and does not affect hardware based traffic routing/forwarding in any way. Typically, the switch examines the received packets in software to check if there is a forwarding entry, create a forwarding entry (e.g., add a L2 MAC address or ARP response), and then either discard the packet or software forward the packet (only occurs during the brief transitional period when the system is actively adding a hardware forwarding entry but the hardware is not yet updated). Processing delays for higher priority packets may occur when the internal CPU queue is continually kept busy handling low priority packets.
This command does not affect the rate limits for control plane packets. It is almost never necessary to use this command to change from the default value. The use of this command should be restricted to situations in which moderate to high rates of unknown unicast/multicast are continually sent to the switch CPU as evidenced by the `show process cpu` command and where the `ipMapForwardingTask` is showing high CPU usage. This occurs most frequently in networks where a high number of ARPs are continually received on untrusted ports, high numbers of L2 stations are timing out and reappearing or multicast flooding is occurring in the network. If problems with L2, L3 or multicast learning occur after changing this value, set the rate limit back to the default value and take other steps to correct or mitigate the underlying network issue directly.

Use the `show system internal pktmgr` command to show the configured value.

**Example**

The following example shows output with higher than normal CPU usage due to packets copied to the software forwarding task.

```
code
console#show process cpu

Memory Utilization Report

status bytes
------- -------
free   1053933568
alloc  673873920

CPU Utilization:

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>5 Secs</th>
<th>60 Secs</th>
<th>300 Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1129</td>
<td>osapiTimer</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>1133</td>
<td>_interrupt_thread</td>
<td>0.09%</td>
<td>0.01%</td>
<td>0.00%</td>
</tr>
<tr>
<td>1137</td>
<td>bcmCNTR.0</td>
<td>0.24%</td>
<td>0.31%</td>
<td>0.31%</td>
</tr>
<tr>
<td>1142</td>
<td>bcmRX</td>
<td>23.00%</td>
<td>27.01%</td>
<td>18.01%</td>
</tr>
<tr>
<td>1147</td>
<td>ipMapForwardingTask</td>
<td>32.97%</td>
<td>37.11%</td>
<td>29.92%</td>
</tr>
<tr>
<td>1155</td>
<td>bcmLINK.0</td>
<td>0.34%</td>
<td>0.36%</td>
<td>0.36%</td>
</tr>
<tr>
<td>1156</td>
<td>cpuUtilMonitorTask</td>
<td>0.09%</td>
<td>0.05%</td>
<td>0.04%</td>
</tr>
<tr>
<td>1170</td>
<td>nim_t</td>
<td>0.09%</td>
<td>0.08%</td>
<td>0.07%</td>
</tr>
<tr>
<td>1208</td>
<td>dot1s_timer_task</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>1222</td>
<td>snoopTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>1291</td>
<td>RMONTask</td>
<td>0.00%</td>
<td>0.02%</td>
<td>0.03%</td>
</tr>
</tbody>
</table>
```
show interfaces

Use the show interfaces command to list the traffic statistics for one or multiple interfaces. If no parameter is given, all interfaces are shown.

Syntax

show interfaces [ interface-id ]

- interface-id—A physical interface id (i.e., a 1G, 10G, or 40G interface) in standard interface format.

Default Configuration

There is no default configuration.

Command Mode

All modes, including Config mode and all config submodes.

User Guidelines

The show interface command shows the actual operational status of the interface, which is not necessarily the same as the configuration.

Input/output rate statistics are collected every 10 seconds.

The link status field shows the hardware status followed by the keepalive status. The hardware status show “Up” when link is detected, “Down” when no link is detected, “Err-disable” when the port is error-disabled, and “Shut” when the port is administratively shut down.

The keepalive status shows “None” when keepalives are disabled or the port is down, “Up” when keepalives are enabled and no loop is detected and “Down” when keepalives are enabled and a loop is detected. Some example values are:

Link Status : ......................... Up/Up
Link detected, keepalives enabled, no loop detected

Link Status : ......................... Shut/None
Port is administratively disabled

Link Status : ......................... Down/None
No link detected

**Link Status** : ......................... Err-disable/Down

Interface is error disabled due to loop detection

**Link Status** : ......................... Err-disable/None

The interface is error disabled due to a cause other than loop detection. The possible causes for error disabled interfaces are:

<table>
<thead>
<tr>
<th>Term</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP inspection</td>
<td>arp-inspection</td>
<td>ARP inspection auto-recovery.</td>
</tr>
<tr>
<td>BPDU Guard</td>
<td>bpduguard</td>
<td>BPDU guard auto-recovery.</td>
</tr>
<tr>
<td>Broadcast Storm</td>
<td>bcast-storm</td>
<td>Broadcast storm auto-recovery.</td>
</tr>
<tr>
<td>BPDU Storm</td>
<td>bpdustorm</td>
<td>BPDU storm auto-recovery.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>denial-of-service</td>
<td>Denial of Service auto-recovery.</td>
</tr>
<tr>
<td>DHCP Rate Limit</td>
<td>dhcp-rate-limit</td>
<td>DHCP rate limit auto-recovery.</td>
</tr>
<tr>
<td>Loop Protection</td>
<td>loop-protect</td>
<td>Loop protection auto-recovery.</td>
</tr>
<tr>
<td>Port MAC Locking</td>
<td>port-security</td>
<td>Port security MAC locking auto-recovery.</td>
</tr>
<tr>
<td>Multicast Storm</td>
<td>mcast-storm</td>
<td>Multicast storm auto-recovery.</td>
</tr>
<tr>
<td>SFP Mismatch</td>
<td>sfp-mismatch</td>
<td>SFP mismatch auto-recovery.</td>
</tr>
<tr>
<td>SFP Plus Mismatch</td>
<td>sfplus-mismatch</td>
<td>SFP+ transceiver inserted in SFP port auto-recovery.</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>spanning-tree</td>
<td>Spanning-tree auto-recovery.</td>
</tr>
<tr>
<td>UDLD</td>
<td>udld</td>
<td>UDLD auto-recovery.</td>
</tr>
<tr>
<td>Unicast Storm</td>
<td>ucast-storm</td>
<td>Unicast storm auto-recovery.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware. Updated in version 6.3.0.1 firmware. Updated in version 6.5 firmware.
Example

The following example shows the output for a 1G interface:

```
console#show interfaces gi1/0/1

Interface Name : ................................ G1/0/1
SOC Hardware Info : ............................ BCM56342_A0
Link Status : .................................. Up/Up
Keepalive Enabled ................................ TRUE
Err-disable Cause : ............................. None
VLAN Membership Mode: ........................ Trunk Mode
VLAN Membership: .............................. (1),2-3,101-113,813,3232
MTU Size : .................................... 1518
Port Mode [Duplex] : .......................... Full
Port Speed : .................................. 1000
Link Debounce Flaps : .......................... 0
Auto-Negotiation Status : ...................... Auto
Burned MAC Address : ......................... 001E.C9DE.B110
L3 MAC Address............................... 001E.C9DE.B112
Sample load interval : ........................ 300
Received Input Rate Bits/Sec : ............... 784
Received Input Rate Packets/Sec : .......... 1
Transmitted Input Rate Bits/Sec : ............ 1344
Transmitted Input Rate Packets/Sec : ....... 1
Total Packets Received Without Errors........ 102792
Unicast Packets Received..................... 0
Multicast Packets Received................... 102792
Broadcast Packets Received................... 0
Total Packets Received with MAC Errors...... 0
Jabbers Received................................ 0
Fragments/Undersize Received.................. 0
Alignment Errors.............................. 0
FCS Errors.................................... 0
Overruns....................................... 0
Total Received Packets Not Forwarded........ 7
Total Packets Transmitted Successfully...... 147070
Unicast Packets Transmitted................... 0
Multicast Packets Transmitted................. 147070
Broadcast Packets Transmitted................ 0
Transmit Packets Discarded.................... 0
Total Transmit Errors.......................... 0
Total Transmit Packets Discarded............. 0
Single Collision Frames....................... 0
Multiple Collision Frames..................... 0
Excessive Collision Frames.................... 0
```
console#show interfaces po1

<table>
<thead>
<tr>
<th>Intf Ports</th>
<th>Ch-Type</th>
<th>Hash</th>
<th>Min-link</th>
<th>Local Prf</th>
<th>TX Util</th>
<th>RX Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>Po1</td>
<td>Active: Te1/0/1, Te1/0/2 Dynamic</td>
<td>7</td>
<td>1</td>
<td>Disabled</td>
<td>432344</td>
<td>83782</td>
</tr>
</tbody>
</table>

Utilization is shown in Mbps.

Hash Algorithm Type
1 - Source MAC, VLAN, EtherType, source module and port Id
2 - Destination MAC, VLAN, EtherType, source module and port Id
3 - Source IP and source TCP/UDP port
4 - Destination IP and destination TCP/UDP port
5 - Source/Destination MAC, VLAN, EtherType, source MODID/port
6 - Source/Destination IP and source/destination TCP/UDP port
7 - Enhanced hashing mode

**show interfaces advertise**

Use the show interfaces advertise command to display information about auto-negotiation advertisement. The display includes the local configuration and link partner advertisement, in addition to the local advertisement.

**Syntax**

show interfaces advertise [{gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The priority resolution field indicates the auto-negotiated link speed and duplex. The clock field indicates whether the local interface has auto-negotiated to clock master or clock slave. When the link is down, the field will show No link.

When the link is down, the Oper Peer Advertisement and Priority Resolution fields will show dashes.
Examples
The following examples display information about auto negotiation advertisement.

Example #1
console#show interfaces advertise

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Neg</th>
<th>Operational Link Advertisement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 10f</td>
</tr>
</tbody>
</table>

Example #2
console#show interfaces advertise gi1/0/1

Port: Gi1/0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
802.3az EEE: Disabled
Clock: Master

<table>
<thead>
<tr>
<th></th>
<th>10000f</th>
<th>1000f</th>
<th>1000h</th>
<th>100f</th>
<th>100h</th>
<th>10f</th>
<th>10h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Local link Advertisement</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Oper Local link Advertisement</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Oper Peer Advertisement</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Priority Resolution</td>
<td>-</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

show interfaces configuration

Use the show interfaces configuration command in User Exec mode to display the configuration for all configured interfaces.

Syntax

show interfaces configuration [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The displayed port configuration information includes the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Description</td>
<td>The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Displays the port Duplex status.</td>
</tr>
<tr>
<td>Speed</td>
<td>Refers to the port speed.</td>
</tr>
<tr>
<td>Neg</td>
<td>Describes the Auto-negotiation status.</td>
</tr>
<tr>
<td>MTU</td>
<td>The Maximum Transmission Unit.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Displays whether the port is enabled or disabled.</td>
</tr>
</tbody>
</table>

**Example**

The following example displays the configuration for all configured interfaces:

```
console#show interfaces configuration gigabitethernet 1/0/1

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>MTU</th>
<th>Admin State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td></td>
<td>Full 1000</td>
<td>Auto 1518</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>
```

**show interfaces counters**

Use the `show interfaces counters` command in User Exec mode to display traffic seen by the interface.
**Syntax**

```
show interfaces counters [errors] [gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port]
```

- **errors**—Show the error counts (frame discards and reasons) in the in and out direction.
- **gigabitethernet**—Shows the traffic for the specified Gigabit Ethernet port.
- **port-channel**—Shows the traffic for the specified port channel port.
- **tengigabitethernet**—Shows the traffic for the specified 10-Gigabit Ethernet port.
- **fortygigabitethernet**—Shows the traffic for the specified 40-Gigabit Ethernet port.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table describes the fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>Counted received octets.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Counted received unicast packets.</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>Counted received multicast packets.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>Counted received broadcast packets.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Counted transmitted octets.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>Counted transmitted unicast packets.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>Counted transmitted multicast packets.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Counted transmitted broadcast packets.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>A count of frames received that are not an integral number of octets in length and do not pass the FCS check.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Counted frames received that are an integral number of octets in length but do not pass the FCS check.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>Counted frames that are involved in a single collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>A count of frames that are involved in a multiple collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Counted times that a collision is detected later than one slot time into the transmission of a packet.</td>
</tr>
<tr>
<td>Excessive Collisions</td>
<td>Counted frames for which transmission fails due to excessive collisions.</td>
</tr>
<tr>
<td>Received packets dropped &gt; MTU</td>
<td>Count of received frames dropped due to frame length greater than the configured MTU.</td>
</tr>
<tr>
<td>Transmitted oversized packets</td>
<td>Count of frames transmission &gt; 1518 octets.</td>
</tr>
<tr>
<td>Internal MAC Rx Errors</td>
<td>A count of frames for which reception fails due to an internal MAC sublayer receive error.</td>
</tr>
<tr>
<td>Received Pause Frames</td>
<td>A count of MAC Control frames received with an opcode indicating the PAUSE operation.</td>
</tr>
<tr>
<td>Transmitted Pause Frames</td>
<td>Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.</td>
</tr>
<tr>
<td>Received PFC Frames</td>
<td>A count of the received Priority Flow Control (PFC) frames.</td>
</tr>
<tr>
<td>Transmitted PFC Frames</td>
<td>A count of the transmitted PFC frames.</td>
</tr>
<tr>
<td>Receive Packets Discarded</td>
<td>Count of frames discarded on receipt due to any reason.</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>Count of packets queued for transmission and discarded for any reason.</td>
</tr>
</tbody>
</table>

**Example**

The following example displays traffic seen by the Ethernet interface:
console>show interfaces counters

<table>
<thead>
<tr>
<th>Port</th>
<th>InTotalPkts</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/13</td>
<td>11447</td>
<td>6867</td>
<td>4580</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/16</td>
<td>51119</td>
<td>12196</td>
<td>38917</td>
<td>6</td>
</tr>
<tr>
<td>Gi1/0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutTotalPkts</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The following example displays counters for Ethernet port Te1/0/1.

```
console(config-if-Te1/0/1)#show interfaces counters tengigabitethernet 1/0/13
```
show interfaces debounce

Use the `show interfaces debounce` command to list the debounce information for one or multiple interfaces. If no parameter is given, all Ethernet interfaces are shown.

**Syntax**

```
show interfaces debounce [ interface-id ]
```

- interface-id—An Ethernet interface identifier (i.e., a 1G, 10G, or 40G Ethernet interface) in standard interface format.

**Default Configuration**

Ethernet interfaces have a 100 ms debounce time enabled.

**Command Mode**

Exec mode, Privileged Exec, Global Configuration and all show modes.
User Guidelines
Use the link debounce time command to configure the debounce time for an interface.

Command History
Introduced in version 6.2.0.1 firmware.

Example
The following example shows the output for representative interfaces.

```
console#show interfaces debounce
Interface Debounce Time (ms) Flaps
--------- ------------------ -------
Gi1/0/1   500                0
```

show interfaces description
Use the show interfaces description command in User Exec mode to display the description for all configured interfaces.

Syntax
```
show interfaces description [gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port]
```

Default Configuration
This command has no default configuration.

Command Mode
User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.
Example
The following example displays the description for all interfaces.

```console
console>show interfaces description
Port    Description
----    ------------------------------------------------
Gi1/0/1 Port that should be used for management only
Gi2/0/1
Gi2/0/2
```

Port    Description
-----    ------------------------------------------------
Po1

show interfaces detail
Use the show interfaces detail command to display detailed status and configuration of the specified interface.

Syntax
```
show interfaces detail interface-id
```
- `interface-id`—An Ethernet interface identifier or port channel identifier.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays detailed status and configuration of the specified interface.

```console
console#show interfaces detail gi1/0/1
Port      Description                 Duplex Speed   Neg  MTU   Admin Link
State State
```
<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>N/A</th>
<th>Unknown</th>
<th>Auto</th>
<th>1518</th>
<th>Up</th>
<th>Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flow Control: Enabled  
Port: Gi1/0/1  
VLAN Membership mode: Access Mode  
Operating parameters:  
PVID: 1  
Ingress Filtering: Enabled  
Acceptable Frame Type: Admit All  
Default Priority: 0  
GVRP status: Disabled  
Protected: Disabled

Port Gi1/0/1 is member in:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>Untagged</td>
<td>Default</td>
</tr>
</tbody>
</table>

Static configuration:  
PVID: 1  
Ingress Filtering: Enabled  
Acceptable Frame Type: Admit All  
Port Gi1/0/1 is statically configured to:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress rule</th>
</tr>
</thead>
</table>

Forbidden VLANs:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
</table>

Port Gi1/0/1 Enabled  
State: Disabled  
Role: Disabled  
Port id: 128.1  
Port Cost: 0  
Port Fast: No (Configured: no)  
Root Protection: No  
Designated bridge Priority: 32768  
Address: 1418.7715.2368  
Designated port id: 0.0  
Designated path cost: 0  
CST Regional Root: 80:00:14:18:77:15:23:68 CST Port Cost: 0  
BFDUs: Sent: 0, Received: 0

**show interfaces status**

Use the `show interfaces status` command to display the status for all configured interfaces.
Syntax
show interfaces status

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
Port channels are only displayed if configured. Use the show interfaces port-channel command to display configured and unconfigured port channels. Interfaces configured as stacking ports will show as detached in the output of the show interfaces status command.

The link state indicates the physical connectivity state of the link. It is possible that the link is connected physically yet frames are not able to pass over the link. Possible causes of this condition are speed or duplex mismatch.

The displayed port status information includes the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port or port channel number. <strong>Oob</strong> means Out-of-Band Management Interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the port. This field may be truncated in the command output.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Displays the port Duplex status.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN membership for the port is enclosed in parentheses. The currently active PVID and Voice VLAN ID, if any, are also shown. In some cases, the PVID assigned may not be the configured PVID, for example, when RADIUS assigns a PVID to the interface.</td>
</tr>
<tr>
<td>Speed</td>
<td>Refers to the port speed.</td>
</tr>
<tr>
<td>Neg</td>
<td>Describes the Auto-negotiation status.</td>
</tr>
<tr>
<td>Link State</td>
<td>Displays the Link status, either <strong>Up</strong> or <strong>Down</strong>.</td>
</tr>
</tbody>
</table>
The following table displays the interface mode codes and VLAN output format for the interface mode:

<table>
<thead>
<tr>
<th>Mode</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>A – Access</td>
<td>Native</td>
</tr>
<tr>
<td>T – Trunk</td>
<td>(Native),List</td>
</tr>
<tr>
<td>D – Dot1q tunnel</td>
<td>Outer</td>
</tr>
<tr>
<td>P – Private VLAN Promiscuous</td>
<td>(Primary), Secondary List</td>
</tr>
<tr>
<td>H–Private VLAN Host</td>
<td>(Primary), Secondary</td>
</tr>
<tr>
<td>G– General</td>
<td>(PVID), All the tagged and untagged VLANs.</td>
</tr>
</tbody>
</table>

**Example**

The following example displays the status for all configured interfaces.

```
console(config-if-Po1)#show interfaces status
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Link</th>
<th>Flow</th>
<th>M</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td>1,3,5,7,9,15,19,25-4093</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>T</td>
<td>(11),1,3,5,7,9,15,19,25-4093</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>G</td>
<td>(1),2,4,6,8,10,14,16,20,22,24</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td></td>
<td>N/A</td>
<td>Unknown</td>
<td>Auto Down</td>
<td>Off</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Oob  Type        Link
---  ----------------  ----
oob Out-Of-Band  Up
show interfaces transceiver

Use the show interfaces transceiver command to display the optic static parameters as well as the Dell EMC qualification.

Syntax

show interfaces transceiver [properties]
  • properties—Displays the static parameters for the optics.

Default Configuration

This command has no default configuration.

Command Modes

User Exec, Privileged Exec modes.

User Guidelines

This command only supports the display of 10G and 40G transceivers.

Example

The following example shows the qualifications status of the optics on the switch.

crash#show interfaces transceiver

<table>
<thead>
<tr>
<th>Port</th>
<th>Dell EMC Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/9</td>
<td>Yes</td>
</tr>
<tr>
<td>Te1/0/11</td>
<td>Yes</td>
</tr>
<tr>
<td>Te1/0/13</td>
<td>N/A</td>
</tr>
<tr>
<td>Te1/0/15</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/17</td>
<td>No</td>
</tr>
</tbody>
</table>

The following example shows static parameters of the optics along with the qualifications status.
console#show interfaces transceiver properties

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Media</th>
<th>Serial Number</th>
<th>Dell EMC Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/9</td>
<td>SFP+</td>
<td>10GBASE-LRM</td>
<td>ANF0L5J</td>
<td>Yes</td>
</tr>
<tr>
<td>Te1/0/11</td>
<td>SFP+</td>
<td>10GBASE-LRM</td>
<td>ANF0L5R</td>
<td>Yes</td>
</tr>
<tr>
<td>Te1/0/13</td>
<td>SFP</td>
<td>1GBASE-SX</td>
<td>PCC1PT5</td>
<td>N/A</td>
</tr>
<tr>
<td>Te1/0/15</td>
<td>SFP+</td>
<td>10GBASE-SR</td>
<td>AD1125A002R</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/17</td>
<td>SFP+</td>
<td>10GBASE-SR</td>
<td>AD0815E00PC</td>
<td>No</td>
</tr>
</tbody>
</table>

**show interfaces trunk**

Use the `show interfaces trunk` command to display active trunk interface information.

**Syntax**

`show interfaces trunk [interface-id]`

- **interface-id**—An Ethernet or port channel interface identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command displays Ethernet interfaces configured in trunk or general mode that are link up. Port channels are also shown if the port channel status is up. The fields displayed are as follows:

- **Port**—The Ethernet or port channel interface name.
- **Description**—The configured port description.
- **Port Chnl**—Shows the port channel if the Ethernet interface is a member of a port channel.
- **M**—The configured mode (T for trunk and G for General).
• Participating VLANs—The participating trunk VLANs with the native VLAN in parentheses. The output shows the port-channel participating VLANs for interfaces bundled in a port-channel.
• STP Forwarding VLANs—The VLANs in the spanning tree forwarding state.

Command History
Command introduced in version 6.5 firmware.

Example
console(config)#show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Port Chnl</th>
<th>M</th>
<th>Participating VLANs</th>
<th>STP Forwarding VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td>T</td>
<td>(1)1-32</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td></td>
<td>T</td>
<td>(10)1-32</td>
<td></td>
<td>10,13,16,19</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td></td>
<td>G</td>
<td>(11)33-64</td>
<td></td>
<td>11,33-64</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td></td>
<td>Po1</td>
<td>T</td>
<td>(11)33-64</td>
<td>1</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td></td>
<td>Po1</td>
<td>T</td>
<td>(11)33-64</td>
<td>11,33-64</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td></td>
<td>Po1</td>
<td>T</td>
<td>(11)33-64</td>
<td>11,33-64</td>
</tr>
<tr>
<td>Po1</td>
<td></td>
<td>T</td>
<td>(11)33-64</td>
<td></td>
<td>11,33-64</td>
</tr>
</tbody>
</table>

show statistics
Use the show statistics command to display detailed statistics for a specific port or for the internal CPU interface.

Syntax
show statistics {gigabitethernet unit/slot/port | switchport | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}

• unit/slot/port—A valid Ethernet interface identifier. See Interface Naming Conventions for interface representation.
• port-channel-number—A port channel identifier.
• switchport—Displays statistics for the internal switch CPU interface.
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
Statistics are only collected for Ethernet interfaces, port-channel interfaces, and the switch CPU interface.

Command History
Modified in version 6.5 firmware.

Examples
The following example shows statistics for port gi1/0/1.

```
console#show statistics gi1/0/1

Total Frames Received (Octets).............. 0
Frames Received 64 Octets.................... 0
Frames Received 65-127 Octets................ 0
Frames Received 128-255 Octets............... 0
Frames Received 256-511 Octets............... 0
Frames Received 512-1023 Octets............... 0
Frames Received 1024-1518 Octets............. 0
Frames Received > 1518 Octets...............  0

Total Frames Received Without Errors........ 0
Unicast Frames Received...................... 0
Multicast Frames Received.................... 0
Broadcast Frames Received................... 0
Jumbo Frames Received........................ 0
Receive Frames Discarded.................... 0

Total Frames Received with MAC Errors....... 0
Jabbers Received............................ 0
Fragments/Undersize Received................ 0
Alignment Errors............................ 0
FCS Errors.................................. 0
Overruns................................... 0
```
Unacceptable Frame Type....................... 0
Received Frames Dropped > MTU................. 0

Total Received Frames Not Forwarded........... 0
802.3x Pause Frames Received.................. 0

Total Frames Transmitted (Octets)............ 0
Frames Transmitted 64 Octets.................. 0
Frames Transmitted 65-127 Octets.............. 0
Frames Transmitted 128-255 Octets............. 0
Frames Transmitted 256-511 Octets............. 0
Frames Transmitted 512-1023 Octets............ 0
Frames Transmitted 1024-1518 Octets......... 0
Frames Transmitted > 1518 Octets............. 0
Max Frame Size................................. 1518

Total Frames Transmitted Successfully........ 0
Unicast Frames Transmitted..................... 0
Multicast Frames Transmitted.................. 0
Broadcast Frames Transmitted.................. 0
Jumbo Frames Transmitted...................... 0

Total Transmit Frames Discarded............... 0
Total Transmit Errors........................... 0
Single Collision Frames........................ 0
Multiple Collision Frames...................... 0
Late Collision Frames........................... 0
Excessive Collision Frames..................... 0

Frames RX and TX 64 Octets.................... 0
Frames RX and TX 65-127 Octets............... 0
Frames RX and TX 128-255 Octets............... 0
Frames RX and TX 256-511 Octets............... 0
Frames RX and TX 512-1023 Octets............. 0
Frames RX and TX 1024-1518 Octets............ 0
Frames RX and TX 1519-2047 Octets............ 0
Frames RX and TX 2048-4095 Octets............ 0
Frames RX and TX 4096-9216 Octets............ 0

802.3x Pause Frames Transmitted............... 0
GVRP PDUs received............................ 0
GVRP PDUs Transmitted........................ 0
GVRP Failed Registrations..................... 0
GMRP PDUs Received............................ 0
GMRP PDUs Transmitted......................... 0
GMRP Failed Registrations..................... 0

BPDUs: Sent: 0, Received: 0
show statistics switchport

Use the show statistics command to display detailed statistics for a specific port or for the entire switch.

Syntax

show statistics {interface-id | switchport}

- interface-id—The interface ID. See Interface Naming Conventions for interface representation.
- switchport—Displays statistics for the entire switch.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

It is possible to enter interface configuration mode from global configuration mode or from interface configuration mode.

RFC Cross Reference

<table>
<thead>
<tr>
<th>Textual Explanation</th>
<th>RFC 2863 MIB Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packets Received (Octets)</td>
<td>ifHCInOctets</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>ifHCInUcastPkts</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>ifHCInMulticastPkts</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>ifHCInBroadcastPkts</td>
</tr>
</tbody>
</table>
Receive Packets Discarded ifInDiscards
Octets Transmitted ifHCOutOctets
Unicast Packets Transmitted ifHCOutUcastPkts
Multicast Packets Transmitted ifHCOutMulticastPkts
Broadcast Packets Transmitted ifHCOutBroadcastPkts
Transmit Packets Discarded ifOutDiscards

Example

The following example shows statistics for the CPU interface.

```
console#show statistics switchport

Total Packets Received (Octets)................ 0
Packets Received Without Error................. 0
Unicast Packets Received....................... 0
Multicast Packets Received..................... 0
Broadcast Packets Received..................... 0
Receive Packets Discarded...................... 0

Octets Transmitted............................. 0
Packets Transmitted Without Errors............. 0
Unicast Packets Transmitted.................... 0
Multicast Packets Transmitted.................. 0
Broadcast Packets Transmitted.................. 0
Transmit Packets Discarded..................... 0

Most Address Entries Ever Used................. 3
Address Entries Currently in Use............... 3

Maximum VLAN Entries........................... 1024
Most VLAN Entries Ever Used.................... 2
Static VLAN Entries............................. 2
Dynamic VLAN Entries........................... 0
VLAN Deletes.................................... 0
Time Since Counters Last Cleared.............. 0 day 18 hr 1 min 59 sec
```
show storm-control

Use the show storm-control command to display the configuration of storm control.

**Syntax**

```
show storm-control [all | {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

The following example shows storm control configurations for a Gigabit Ethernet port. The second example shows flow control mode status.

```
console#show storm-control
802.3x Flow Control Mode....................... Disable

console#show storm-control gigabitethernet 1/0/1

中枢 Bcast Bcast Mcast Mcast Ucast Ucast Flow
Port Mode Level Mode Level Mode Level Ctrl
---------- -------- --------- -------- --------- -------- --------- --------
Gi1/0/1    Enable   90        Enable   5       Enable   10       Enabled
```

```
switch-top(config)#show storm-control all

中枢 Bcast Bcast Mcast Mcast Ucast Ucast Flow
Port Mode Level Mode Level Mode Level Ctrl
---------- -------- --------- -------- --------- -------- --------- --------
Gi1/0/1    Enable   90        Enable   5       Enable   10       Enabled
```
show storm-control action

Use the show storm-control action command to display the storm control action configuration for one or all interfaces.

Syntax

show storm-control action {all | interface-id}

- all — Show the storm control action configuration for all interfaces.
- interface-id — An Ethernet interface on which storm control is enabled.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode and all show modes

User Guidelines

This command has no user guidelines.

Examples

carlete#show storm-control action all

<table>
<thead>
<tr>
<th>Port</th>
<th>Bcast</th>
<th>Mcast</th>
<th>Ucast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Gi1/0/2
Gi1/0/3
Gi1/0/4
Gi1/0/5
Gi1/0/6
Gi1/0/7
Gi1/0/8
shutdown

Use the shutdown command in Interface Configuration mode to disable an interface. To restart a disabled interface, use the no form of this command.

Syntax

```
shutdown
no shutdown
```

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Examples

The following example disables Gigabit Ethernet port 1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)# shutdown
```

The following example reenables Gigabit Ethernet port 1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)# no shutdown
```

speed

Use the speed command in Interface Configuration mode to configure the speed of a given Ethernet interface. To restore the default, use the no form of this command.

Syntax

```
speed {10 | 100 | 1000 | 10000 | 40000 | auto [10 | 100 | 1000 | 2500 | 5000 | 10000]}
no speed
```
• 10—Configures the port to 10 Mbps operation.
• 100—Configures the port to 100 Mbps operation.
• 1000—Configures the port to 1000 Mbps operation.
• 10000—Configures the port to 10 Gbps operation.
• 40000—Configures the port to 40 Gbps operation.
• auto—The port automatically negotiates the highest common speed with the port at the other end of the link. If you use the 10, 100, 1000, 2500, 5000, or 10000 keywords with the auto keyword, the port only advertises the specified speeds.

Default Configuration
Auto-negotiation is enabled by default on copper ports and SFP ports.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
Not all interfaces are capable of supporting all speeds. Refer to the Hardware Overview section of the Users Configuration Guide for a description of the capabilities of a particular interface.

Use the auto parameter to enable auto-negotiation on an interface. Auto-negotiation on copper interfaces selects a clock master, performs link training to tune the pre-emphasis settings to the individual switch and cable, negotiates the internal media, and may enable a decision feedback equalizer (DFE) to correct burst errors if the PHY has the capability. To disable auto-negotiation on a port, it is necessary to enter the speed command without using the auto parameter. Disabling auto-negotiation on 1G copper ports may lead to random frame loss as the clock master and media have not been arbitrated by the auto-negotiation process. Auto-negotiation is required on 2.5G/5G/10G/40G copper ports and is always recommended for copper ports regardless of the speed setting. SFP+ ports utilizing a copper DAC cable are considered copper ports. Auto-negotiation is also required on 1000Base-X ports (including SFP fiber ports.)
When the auto parameter is configured with a set of speeds, only those speeds are advertised during auto-negotiation. Alternatively, if no speed arguments are configured, then all the speeds which the port is capable of supporting are advertised. Not all ports support all speeds, even if they are available in the command. Entering an unsupported speed will produce the following error message: 

An invalid interface has been used for this function.

Fiber ports (other than 1000Base-X) do not support auto-negotiation and therefore require the operator to enter the speed command with the desired operating rate. The link partner must be similarly configured. SFP+/QSFP fiber ports using fiber media do not support auto-negotiation, although it should be enabled when using Direct Attach Copper cables if the link partner also supports auto-negotiation. 1G SFP fiber ports should have auto-negotiation enabled. SFP transceivers in an SFP+ port should have auto-negotiation enabled. The default behavior is to enable auto-negotiation when an SFP transceiver is inserted into an SFP+ port, unless a fixed speed is configured.

Likewise, SFP+ ports connected via copper Direct Attach Cables should have auto-negotiation enabled if the link partner is also capable of performing auto-negotiation. If the link partner cannot perform auto-negotiation, then a fixed speed must be utilized. In all cases, the link partners need compatible settings, e.g., both sides must be set to use auto-negotiation or a fixed speed. In the case of a fixed speed link, both sides must be set to the same speed.

Failure to set both sides of a link to the same speed/duplex values (auto-negotiation disabled) or compatible speed/duplex values (auto-negotiation enabled) may give a false link-up indication when configured or when the link is brought up (no shut). Setting one end of a link to auto-negotiate and the link partner to a fixed speed is not supported. Disabling auto-negotiation on interfaces that require it, for example, 1000BASE-X or 1G/10G copper interfaces, is not supported.

Example

The following example configures Gigabit Ethernet port 1/0/5 to advertise 100-Mbps operation only via auto-negotiation.

```
class (config) #interface gigabitethernet 1/0/5
console(config-if)# speed auto 100
```
Command History
The speed 10000 syntax was introduced in the 6.3.6 release.
The 2500 and 5000 speeds were introduced in the 6.3.5 release. The
description was updated in the 6.4 release.

switchport protected

Use the switchport protected command in Interface Configuration mode to
configure a protected port. The groupid parameter identifies the set of
protected ports to which this interface is assigned. You can only configure an
interface as protected in one group. You are required to remove an interface
from one group before adding it to another group.

Port protection occurs within a single switch. Protected port configuration
does not affect traffic between ports on two different switches. No traffic
forwarding is possible between two protected ports. Ports in a protected group
will not forward traffic to other ports in the group.

Syntax
switchport protected groupid
no switchport protected
  • groupid--Identifies which group this port will be protected in. (Range: 0-2)

Default Configuration
No protected switchports are defined.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
When an interface is enabled for routing using the interface vlan command,
the port will no longer be operationally enabled as a protected port on the
interface. Likewise, making an interface a member of a LAG or a probe
(monitor session or RSPAN destination) port operationally disables port
protection.
Example
The following example configures Ethernet port 1/0/1 as a member of protected group 1.

```
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)#switchport protected 1
```

**switchport protected name**

Use the `switchport protected name` command in Global Configuration mode to add the port to the protected group 1 and also sets the group name to “protected”.

**Syntax**

```
switchport protected groupid name name
no switchport protected groupid name
```

- `groupid` — Identifies which group the port is to be protected in. (Range: 0–2)
- `name` — Name of the group. (Range: 0-32 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example assigns the name “protected” to group 1.

```
console(config)#switchport protected 1 name protected
```
show switchport protected

Use the show switchport protected command to display the status of all the interfaces, including protected and unprotected interfaces.

Syntax
show switchport protected groupid
  • groupid — Identifies which group the port is to be protected in.
    (Range: 0–2)

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example identifies test as the protected group.

console#show switchport protected 0
Name......................................... test

show system mtu

Use the show system mtu command to display the configured MTU. The MTU is set using the global system jumbo mtu command. This command deprecates the show interfaces mtu command.

Syntax
show system mtu

Default Configuration
The default mtu size is 1518 bytes (1522 bytes for VLAN tagged frames).
**Command Modes**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no usage guidelines.

**Example**
```
console #show system mtu
```
System Jumbo MTU size is 9216 bytes

**system jumbo mtu**
Use the `system jumbo mtu` command to globally configure the link Maximum Transmission Unit (MTU) on all interfaces, IP/IPv6 interfaces, VLAN interfaces, and port channel interfaces for forwarded and system-generated frames. The link MTU is the size of the largest Ethernet frame that can be transmitted on an interface without fragmentation. Frames received on an interface are dropped if they exceed the link MTU. Frames larger than this size generated by the system are fragmented before transmission.

This command deprecates the `mtu`, `ip mtu`, and `ipv6 mtu` commands.

Use the `no` form of the command to reset the MTU to the default.

**Syntax**
```
system jumbo mtu frame size
no system jumbo mtu
```

```
• frame size —The maximum frame size, in bytes, received by the system which is not forwarded.
```

**Default Configuration**
The default MTU size is 1518 bytes (1522 bytes for VLAN tagged frames).

**Command Modes**
Global Configuration mode
User Guidelines

Dell EMC Networking N-Series switches do not fragment received packets. The IPv4 and IPv6 MTU are set to the link MTU minus 18 bytes. IP packets forwarded in software are dropped if they exceed the IP MTU. Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtuignore` command).

The allowed range is 1298 to 9216. This allows for configuration of an IPv4 and IPv6 MTU of 1280 to 9198.

In conformance with RFC 2460, the system performs IPv6 path MTU discovery for IPv6 packets originated by the switch. This may result in individual connections using an IPv6 MTU less than that configured by the network operator.
Ethernet CFM Commands

Dell EMC Networking N4000 Series Switches

Connectivity Fault Management (CFM) is the OAM Protocol provision for end-to-end service layer OAM in carrier Ethernet networks. CFM provides mechanisms to support the operator in performing connectivity checks, fault detection, fault verification and isolation, and fault notification per service in the network domain of interest. Unlike Ethernet OAM defined in IEEE 802.3ah, where the faults are detected and notified on a single point-to-point IEEE Std. 802.3 LAN, this capability deals with the fault diagnosis at service layer across networks comprising multiple LANs, including LANs other than 802.3 media. Refer to IEEE 802.1ag for an explanation of CFM. Typically, the MEP ID and maintenance association levels are assigned by the top level network service provider.

Dell EMC Networking CFM is only available on the N4000 series switches. CFM is not compatible with iSCSI optimization. Disable iSCSI optimization before enabling CFM.

Dell EMC Networking CFM supports the following functionality:

- Path discovery (linktrace message)
- Fault detection (continuity check message)
- Fault verification and isolation (loopback and linktrace messages)
- Fault notification (alarm indication signal or SNMP trap)

Commands in this Section

This section explains the following commands:

- `ethernet cfm domain`  
- `ping ethernet cfm`  
- `service`  
- `traceroute ethernet cfm`  
- `ethernet cfm cc level`  
- `show ethernet cfm errors`  
- `ethernet cfm mep level`  
- `show ethernet cfm domain`  
- `ethernet cfm mep enable`  
- `show ethernet cfm maintenance-points`  
- `local`
Use the `ethernet cfm domain` command in Global Configuration mode to enter into Maintenance Domain Configuration mode for an existing domain. Use the optional level parameter to create a domain and enter into maintenance domain Configuration mode. In maintenance domain Configuration mode, maintenance associations are created and per-maintenance domain services can be configured. Use the `no` form of the command to delete a maintenance domain.

**Syntax**

```
ethernet cfm domain domain-name [level 0-7]
```

- `domain-name`—Name of the maintenance domain. Alphanumeric string of up to 43 characters.

**Default Configuration**

No CFM domains are preconfigured.

**Command Mode**

Global Configuration mode

**User Guidelines**

Each domain must have a unique name and level, for example, one cannot create a domain qwerty at level 2 if domain qwerty already exists at level 1. Likewise, one cannot create a domain dvorak at level 2 if a domain of any name exists at level 2.

**Example**

In this example, a domain “vin” is created at level 1.

```
console(config)#ethernet cfm domain vin level 1
```
**service**

Use the `service` command in Maintenance Domain Configuration mode to associate a VLAN with a maintenance domain. Use the `no` form of the command to remove the association.

**Syntax**

```
service service-name vlan vlan-id
```

- `service-name`—Unique service identifier.
- `vlan-id`—VLAN ID representing a service instance that is monitored by this maintenance association. The range is 1-4093.

**Default Configuration**

No VLANs are associated with a maintenance domain by default.

**Command Mode**

Maintenance Domain Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-cfm-mdomain)# service serv1 vlan 10
```

**ethernet cfm cc level**

Use the `ethernet cfm cc level` command in Global Configuration mode to initiate sending continuity checks (CCMs) at the specified interval and level on a VLAN monitored by an existing domain. Use the `no` form of the command to cease send CCMs.

**Syntax**

```
ethernet cfm cc level 0-7 vlan vlan-id interval secs
```

- `ethernet cfm cc level`—Command to initiate sending CCMs.
- `0-7`—Level of CCMs.
- `vlan vlan-id`—VLAN ID to monitor.
- `interval secs`—Interval and level to send CCMs.
• vlan-id—VLAN ID representing a service instance that is monitored by this maintenance association. The range is 1-4093.
• secs—Time interval between successive transmissions. The range is 1, 10, 60, and 600 seconds. The default is 1 second.

**Default Configuration**
CCMs are not sent by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
```
console(config)#ethernet cfm cc level 1 vlan 15 interval 10
```

**ethernet cfm mep level**
Use the `ethernet cfm mep level` command in Interface Configuration mode to create a Maintenance End Point (MEP) on an interface at the specified level and direction. MEPs are configured per Maintenance Association per Maintenance Domain. Use the `no` form of the command to delete a MEP.

**Syntax**
```
ethernet cfm mep level 0-7 direction up|down mpid 1-8191 vlan vlan-id
```
• level—Maintenance association level
• direction—Up indicates the MEP is facing towards Bridge Relay Entity. Down indicates the MEP is facing towards the LAN.
• mpid—Maintenance entity identifier
• vlan-id—VLAN on which the MEP operates. The range is 1-4093.

**Default Configuration**
No MEPs are preconfigured.
Command Mode
Interface Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example creates a maintenance endpoint at level 1 with mpid 1010 on vlan 10.

```
console(config-if-Gi1/0/3)#ethernet cfm mep level 1 direction up mpid 1010 vlan 10
```

**ethernet cfm mep enable**

Use the `ethernet cfm mep enable` command in Interface Configuration mode to enable a MEP at the specified level and direction. Use the `no` form of the command to disable the MEP.

**Syntax**

```
ethernet cfm mep enable level 0-7 vlan vlan-id mpid 1-8191
```

- **level**—Maintenance association level
- **mpid**—Maintenance entity identifier
- **vlan**—VLAN on which the MEP operates. The range is 1-4093.

**Default Configuration**

No MEPs are preconfigured.

**Command Mode**

Interface Configuration mode

**User Guidelines**

The maintenance domain must exist for it to be enabled.
Example

The following example enables a maintenance endpoint at level 1 with mpid 1010 on vlan 10.

```
console(config-if-Gi1/0/3)#ethernet cfm mep enable level 1 vlan 10 mpid 1010
```

**ethernet cfm mep active**

Use the `ethernet cfm mep active` command in Interface Configuration mode to activate a MEP at the specified level and direction. Use the `no` form of the command to deactivate the MEP.

**Syntax**

```
ethernet cfm mep active level 0-7 vlan vlan-id mpid 1-8191
```

- **level**—Maintenance association level
- **mpid**—Maintenance entity identifier
- **vlan**—VLAN on which the MEP operates. The range is 1-4093.

**Default Configuration**

No MEPs are preconfigured.

**Command Mode**

Interface Configuration

**User Guidelines**

This command has no user guidelines.

**ethernet cfm mep archive-hold-time**

Use the `ethernet cfm mep archive-hold-time` command in Interface Configuration mode to maintain internal information on a missing MEP. Use the `no` form of the command to return the interval to the default value.

**Syntax**

```
ethernet cfm mep archive-hold-time hold-time
```
• **hold-time**—The time in seconds to maintain the data for a missing MEP before removing the data. The default value is 600 seconds.

**Default Configuration**
No MEPs are preconfigured.

**Command Mode**
Interface Configuration

**User Guidelines**
The hold time should generally be less than the CCM message interval.

**Example**
The following example sets the hold time for maintaining internal information regarding a missing MEP.

```console
console(config)#ethernet cfm mep archive-hold-time 1200
```

**ethernet cfm mip level**
Use the `ethernet cfm mip level` command in Interface Configuration mode to create a Maintenance Intermediate Point (MIP) at the specified level. The MEPs are configured per Maintenance Domain per interface. Use the `no` form of the command to delete a MIP.

**Syntax**
```
ethernet cfm mip level 0-7
```

• **level**—Maintenance association level

**Default Configuration**
No MIPs are preconfigured.

**Command Mode**
Interface Configuration
User Guidelines

Refer to IEEE 802.1ag for an explanation of maintenance association levels. Typically, this value is assigned by the top level network service provider.

Example

console(config-if-Gi1/0/1)# ethernet cfm mip level 7

ping ethernet cfm

Use the ping ethernet cfm command to generate a loopback message (LBM) from the configured MEP.

Syntax

ping ethernet cfm {mac mac-addr | remote-mpid 1-8191} {domain domain name | level 0-7} vlan vlan-id mpid 1-8191 [count 1-255]

- level—Maintenance association level
- mac-addr—The destination MAC address for which the connectivity needs to be verified. Either MEP ID or the MAC address option can be used.
- remote-mpid—The MEP ID for which connectivity is to be verified; i.e. the destination MEP ID.
- domain—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
- vlan-id—A VLAN associated with the maintenance domain. Range: 1-4093.
- mpid—The MEP ID from which the loopback message needs to be transmitted.
- count—The number of LBMs to be transmitted. The default number is 1.

Default Configuration

By default, this command will transmit one loopback message with a time-out of five seconds.

Command Mode

Privileged Exec
User Guidelines
This command has no user guidelines.

Example
console #ping ethernet cfm mac 00:11:22:33:44:55 level 1 vlan 10 mpid 1 count 10

traceroute ethernet cfm
Use the traceroute ethernet command to generate a link trace message (LTM) from the configured MEP.

Syntax
traceroute ethernet cfm {mac mac-addr| remote-mpid 1-8191} {domain domain name | level 0-7} vlan vlan-id mpid 1-8191 [ttl 1-255]

- level—Maintenance association level
- mac-addr—The destination MAC address for which the connectivity needs to be verified. Either MEP ID or the MAC address option can be used.
- remote-mpid—The MEP ID for which connectivity is to be verified; i.e. the destination MEP ID.
- domain—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
- vlan-id—A VLAN associated with the maintenance domain. Range: 1-4093.
- mpid—The MEP ID from which the loopback message needs to be transmitted.
- ttl—The number of hops over which the LTM is expected to be transmitted. The default number is 64.

Default Configuration
By default, the traceroute command will send loopback trace messages with a TTL of 64.

Command Mode
Privileged Exec
**User Guidelines**
This command has no user guidelines.

**Example**
```
console # traceroute ethernet cfm remote-mpid 32 level 7 vlan 11 mpid 12
```

**show ethernet cfm errors**
Use the `show ethernet cfm errors` command to display the cfm errors.

**Syntax**
```
show ethernet cfm errors {domain domain-id | level 0-7}
```
- **level**—Maintenance association level
- **domain**—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
- **Level**—The maintenance association level
- **SVID**—The service identifier
- **MPID**—The maintenance endpoint identifier
- **DefRDICcm**—A remote MEP reported the RDI bit in a CCM.
- **DefMACStatus**—Some remote MEP reported its Interface Status TLV as something other then isUp.
- **DefRemoteCCM**—The MEP did not receive valid CCMs from at least one of the remote MEPs
- **DefErrorCCM**—The MEP has received at least one invalid CCM whose CCM interval has not yet timed out.
• DevXconCCM—The MEP has received at least one CCM from either another MAID or a lower MD level whose CCM interval has not yet timed out.

Example

```
console#show ethernet cfm errors
```

```
----- ---- ---- --------- ------------ ------------ ----------- ----------
Level SVID MPID DefRDICcm DefMACStatus DefRemoteCCM DefErrorCCM DefXconCCM
----- ---- ---- --------- ------------ ------------ ----------- ----------
show ethernet cfm domain

Use the `show ethernet cfm domain` command to display the configured parameters in a maintenance domain.

Syntax

```
show ethernet cfm domain {brief | domain-id}
```

- **domain**—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

```
console # show Ethernet cfm domain domain1
```

```
Domain Name : domain1
Level       : 1
Total Services : 1
---- ----------------------------------- ------------------
VLAN ServiceName                         CC-Interval (secs)
---- ----------------------------------- ------------------
10 serv1                                  1
```
show ethernet cfm maintenance-points local

Use the `show ethernet cfm maintenance-points local` command to display the configured local maintenance points.

**Syntax**

```
show ethernet cfm maintenance-points local {level 0-7 | interface interface-id | domain domain-name}
```

- **level**—Maintenance association level
- **domain**—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
- **interface-id**—Show all MPs associated with the interface. This command accepts Ethernet interface identifiers and port channel interface identifiers.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

Refer to IEEE 802.1ag for an explanation of the maintenance association level and MEP ID. Typically, these are assigned by the top level network service provider.

- MPID—The maintenance endpoint identifier
- Level—The MEP level
- Type—Maintenance endpoint (MEP) or maintenance intermediate point (MIP)
- VLAN—The configured VLAN id
- Port—The port on which the MEP association is configured
- Direction—(Up)stream or (Do)wnstream
- CC Transmit—Continuity check enabled
- MEP-Active—The MEP administrative status
- Operational Status—The MEP operational status
- MAC—The MAC address associated with the MEP.

**Example**

```
show ethernet cfm maintenance-points local level 1
```

```
MPID Level Type VLAN Port Direction Transmit Active Status
---- ----- ---- ---- ------ -------- ------ ----------- ----- 
1 1 MEP 10 Gi1/0/1 UP Enabled True 00:02:bc:02:02:02
```

```
show ethernet cfm maintenance-points remote
```

Use the `show ethernet cfm maintenance-points remote` command to display the configured remote maintenance points.

**Syntax**

```
show ethernet cfm maintenance-points remote {level 0-7 | domain domain-name | detail [mac mac-address | mep mpid] [domain domain-name | level 0-7] [vlan vlan-id]}
```

- **domain**—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
- **level**—Maintenance association level
- **mac-addr**—The destination MAC address for which the connectivity needs to be verified. Either MEP ID or the MAC address option can be used.
- **vlan-id**—A VLAN associated with the maintenance domain. Range: 1-4093.
- **mpid**—The MEP ID from which the loopback message needs to be transmitted.

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
Refer to IEEE 802.1ag for an explanation of the maintenance association level and MEP ID. Typically, these are assigned by the top level network service provider.

- MEP Id—Local MEP identifier
- RMep Id—Remote MEP identifier
- Level—Connectivity association level
- MAC—Destination MAC address
- VLAN—VLAN on which the MEP is configured
- Expiry timer—The configured MEP expiry timer
- Service Id—The configured service identifier

**Example**
```
console# show ethernet cfm maintenance-points remove level 1
```

<table>
<thead>
<tr>
<th>MEP Id</th>
<th>RMEP Id</th>
<th>Level</th>
<th>MAC</th>
<th>VLAN</th>
<th>Expiry Timer(sec)</th>
<th>Service Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>00:11:22:33:44:55</td>
<td>10</td>
<td>25</td>
<td>serv1</td>
</tr>
</tbody>
</table>

**show ethernet cfm statistics**
Use the `show ethernet cfm maintenance-points remote` command to display the CFM statistics.

**Syntax**
```
show ethernet cfm statistics [domain domain-name | level 0-7]
```
- domain-name—Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
- level—Maintenance association level
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
Refer to IEEE 802.1ag for an explanation of the maintenance association level. Typically, maintenance levels are assigned by the top level network service provider.

- Out-of-sequence CCM's received—Count of the out-of-sequence continuity check messages (CCM's) received
- CCM's transmitted—Count of the CCMs transmitted
- In order Loopback replies received—Count of the in order loopback replies received
- Bad MSDU Loopback Replies received—Count of the number of loopback replies received with a MAC Service Data Unit that did not match the corresponding LBM
- Unexpected LTR's received—A count of the number of Link Trace Replies for which no LTM was sent

Example

```
show Ethernet cfm statistics [domain <domain-name> | level <0-7>]
```

```
Console# show ethernet cfm statistics

-----------------------------------------------
Statistics for 'Domain: domain1, Level: 1, Vlan: 11, MEP Id: 1'
-----------------------------------------------
Out-of-sequence CCM's received : 0
CCM's transmitted : 259
In-order Loopback Replies received : 5
Out-of-order Loopback Replies received: 0
Bad MSDU Loopback Replies received : 0
Loopback Replies transmitted : 5
Unexpected LTR's received : 0
-----------------------------------------------
```
Statistics for 'Domain: domain1, Level: 1, Vlan: 11, MEP Id: 2'
------------------------------------------------------------------
Out-of-sequence CCM's received : 0
CCM's transmitted             : 1
In-order Loopback Replies received : 5
Out-of-order Loopback Replies received : 5
Bad MSDU Loopback Replies received : 0
Loopback Replies transmitted  : 0
Unexpected LTR's received    : 0
------------------------------------------------------------------
Statistics for 'Domain: domain1, Level: 1, Vlan: 11, MEP Id: 3'
------------------------------------------------------------------
Out-of-sequence CCM's received : 0
CCM's transmitted             : 1
In-order Loopback Replies received : 0
Out-of-order Loopback Replies received : 0
Bad MSDU Loopback Replies received : 0
Loopback Replies transmitted  : 5
Unexpected LTR's received    : 0
Green Ethernet Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dell EMC Networking switches support various Green Ethernet modes, i.e., power saving modes, namely:

- Energy-Detect Mode
- Energy Efficient Ethernet

These modes can enable significant operational cost reductions through direct power savings and reducing cooling costs. Green mode commands are only valid for copper Ethernet interfaces.

Energy-Detect Mode

With this mode enabled, when the port link is down the PHY automatically goes down for short periods of time and then wakes up periodically to check for link pulses. This reduces power consumption when no link partner is present. This feature is currently available only on GE copper ports.

Energy Efficient Ethernet

Energy Efficient Ethernet (EEE) combines the MAC with a family of PHYs that support operation in a Low Power Mode as defined by the IEEE 802.3az Energy Efficient Ethernet Task Force. Lower Power Mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. Transition to Low Power Mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from Low Power Mode. Transition time is transparent to upper layer protocols and applications. LLDP must be enabled in order to EEE to operate on a link. This feature is currently available only on copper ports.

Commands in this Section

This section explains the following commands:

clear counters  show green-mode interface-id
green-mode energy-detect

This command enables a Dell EMC proprietary mode of power reduction on ports that are not connected to another interface. Use the green-mode energy-detect command in Interface Configuration mode to enable energy-detect mode on an interface or all the interfaces. Energy-detect mode is enabled by default on 1G copper interfaces and enabled by default on 10G copper interfaces.

On combo ports, it is possible to configure energy-detect mode even if the fiber port is enabled. If enabled, energy-detect mode will become active when the copper port is used.

Use the no form of the command to disable energy-detect mode on the interface(s).

Syntax

green-mode energy-detect

do green-mode energy-detect

Default Configuration

On N1100-ON, N1500, N2000, N2100-ON, N3000, and N3100-ON switches, energy-detect is enabled by default. Energy detect mode is enabled by default and cannot be disabled on N4000 10G copper interfaces.

Command Mode

Interface Configuration mode

User Guidelines

This command is available in Ethernet interface configuration mode. Cable diagnostics (show copper-ports tdr command) may give misleading results if green mode is enabled on the port. Disable green mode prior to running any cable diagnostics. EEE and energy-detect modes are only supported on N4000...
Series 10G ports and on N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON 1G copper ports. Energy-detect mode is always enabled on N4000 series 10G ports and cannot be disabled. An error message (Unable to set energy-detect mode) will be displayed if the user attempts to configure energy-detect on a 10G port on a N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON series switch.

**green-mode eee**

Use the `green-mode eee` command in Interface Configuration mode to enable EEE low power idle mode on an interface. The command enables both send and receive sides of a link to disable some functionality for power savings when lightly loaded. The transition to Low Power Idle mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from Low Power Idle mode.

On combo ports, eee mode can be enabled even if the port is using the fiber interface. If enabled, eee mode is only active when the copper interface is active.

Use the `no` form of the command to disable the feature.

**Syntax**

```
green-mode eee
no green-mode eee
```

**Default Configuration**

The default value is `Enabled`.

**Command Mode**

Interface Configuration

**User Guidelines**

This command is available in Ethernet interface configuration mode. Cable diagnostics (`show copper-ports` commands) may give misleading results if green mode is enabled on the port. Disable green mode prior to running any
cable diagnostics. EEE mode is supported on N4000 series 10G copper ports and on N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON 1G copper interfaces.

**green-mode eee \{ tx-idle-time | tx-wake-time \}**

Use the **green-mode eee \{tx-idle-time | tx_wake-time\}** command in Interface Configuration mode to control the transmit idle and wake time parameters on an interface.

Use the **no** form of the command to return the configuration to the default.

**Syntax**

- `green-mode eee tx-idle-time <600-4294967295>`
- `green-mode eee tx-wake-time <0-65535>`
- `no green-mode eee \{tx-idle-time|tx-wake-time\}`

**Default Configuration**

By default, the transmit idle time is 600 micro-seconds and the transmit wake time is 8 micro-seconds.

**Command Mode**

Interface Configuration mode, Interface Range Configuration mode

**User Guidelines**

The tx-idle-time parameter sets the amount of time the link must be idle before transitioning to the low power idle state. The tx-wake-time configures the delay before transitioning to the active state (and transmitting the pending packet) after transmitting a wake symbol to the link partner. The transmit idle time and transmit wake time are configured in micro-seconds.

The default values are recommended unless there is good reason to adjust them. Excessive wake times may cause link congestion. Excessive idle times will reduce the savings from low power idle mode.
This command is available in Ethernet interface configuration mode for copper ports that are EEE capable. Configuring the values on interfaces that do not support EEE will return an error.

**Command History**
Syntax added in 6.4 release.

**clear green-mode statistics**
Use the `clear green-mode statistics` command to clear:
- The EEE LPI event count, and LPI duration
- The EEE LPI history table entries
- The Cumulative Power savings estimates for a specified interface or for all the interfaces based upon the argument.

**Syntax**
```
clear green-mode statistics {interface-id | all}
```
- interface-id—An Ethernet interface identifier. See Interface Naming Conventions for interface representation.
- all—All Ethernet interfaces.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec

**User Guidelines**
This command has no user guidelines.

**green-mode eee-lpi-history**
Use the `green-mode eee-lpi-history` command in Global Configuration mode to configure the Global EEE LPI history collection interval and buffer size. This value is applied globally on all interfaces on the stack. LPI history is only
collected on combo ports when the copper port is enabled. Use the no form of the command to set the sampling interval or max-samples values to the default.

**Syntax**

```
green-mode eee-lpi-history {sampling-interval 30 sec – 36000 sec | max-samples 1 - 168}
```

- **sampling-interval**—The interval in seconds at which power consumption data needs to be collected.
- **max-samples**—Maximum number of samples to keep.

**Default Configuration**

The sampling-interval default value is 3600 seconds and the max-samples default value is 168.

**Command Mode**

Global Configuration

**User Guidelines**

EEE and energy-detect modes are only supported on N4000 series 10G copper ports and on N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON 1G copper ports.

**Examples**

Use the command below to set the EEE LPI History sampling interval to the default.

```
console(config)# no green-mode eee-lpi-history sampling-interval
```

Use the command below to set the EEE LPI History max-samples to the default.

```
console(config)# no green-mode eee-lpi-history max-samples
```
show green-mode interface-id

Use the show green-mode interface-id command to display the green-mode configuration and operational status of the port. This command is also used to display the per port configuration and operational status of the green-mode. The status is shown only for the modes supported on the corresponding hardware platform whether enabled or disabled.

Syntax

show green-mode interface-id

- interface-id—An Ethernet interface identifier. See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

This command output provides the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Detect</td>
<td></td>
</tr>
<tr>
<td>Energy-detect admin mode</td>
<td>Energy-detect mode is enabled or disabled.</td>
</tr>
<tr>
<td>Energy-detect operational status</td>
<td>Energy detect mode is currently active or inactive. The energy detect mode may be administratively enabled, but the operational status may be inactive. The reasons for the operational status are described below.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reason for Energy-detect current</td>
<td>The energy detect mode may be administratively enabled, but operational status may be inactive. The possible reasons are:</td>
</tr>
<tr>
<td>operational status</td>
<td>1 Port is currently operating in the fiber mode</td>
</tr>
<tr>
<td></td>
<td>2 Link is up.</td>
</tr>
<tr>
<td></td>
<td>If the energy-detect operational status is active, then the reason field shows up as:</td>
</tr>
<tr>
<td></td>
<td>1 No energy Detected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEE Admin Mode</td>
<td>EEE Admin Mode is enabled or disabled.</td>
</tr>
<tr>
<td>Rx Low Power Idle Event Count</td>
<td>This field is incremented each time MAC RX enters LP IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.</td>
</tr>
<tr>
<td>Rx Low Power Idle Duration (μSec)</td>
<td>This field indicates duration of Rx LPI state in 10us increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.</td>
</tr>
<tr>
<td>Tx Low Power Idle Event Count</td>
<td>This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.</td>
</tr>
<tr>
<td>Rx Low Power Idle Duration (μSec)</td>
<td>This field indicates duration of Tx LPI state in 10us increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.</td>
</tr>
<tr>
<td>Tw_sys_tx (μSec)</td>
<td>Integer that indicates the value of Tw_sys that the local system can support. This value is updated by the EEE DLL Transmitter state diagram. This variable maps into the aLldpXdot3LocTxTwSys attribute.</td>
</tr>
<tr>
<td>Tw_sys Echo (μSec)</td>
<td>Integer that indicates the remote system’s Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system. This value maps into the aLldpXdot3LocTxTwSysEcho attribute.</td>
</tr>
<tr>
<td>Tw_sys rx (μSec)</td>
<td>Integer that indicates the value of Tw_sys that the local system requests from the remote system. This value is updated by the EEE Receiver L2 state diagram. This variable maps into the aLldpXdot3LocRxTwSys attribute.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tw_sys_rx Echo (μSec)</td>
<td>Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support. This value maps into the aLldpXdot3LocRxTwSysEcho attribute.</td>
</tr>
<tr>
<td>Fallback Tw_sys (μSec)</td>
<td>Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system. This value is updated by the local system software.</td>
</tr>
<tr>
<td>Remote Tw_sys_tx (μSec)</td>
<td>Integer that indicates the value of Tw_sys that the remote system can support. This value maps from the aLldpXdot3RemTxTwSys attribute.</td>
</tr>
<tr>
<td>Remote Tw_sys Echo (μSec)</td>
<td>Integer that indicates the value Transmit Tw_sys echoed back by the remote system. This value maps from the aLldpXdot3RemTxTwSysEcho attribute.</td>
</tr>
<tr>
<td>Remote Tw_sys_rx (μSec)</td>
<td>Integer that indicates the value of Tw_sys that the remote system requests from the local system. This value maps from the aLldpXdot3RemRxTwSys attribute.</td>
</tr>
<tr>
<td>Remote Tw_sys_rx Echo (μSec)</td>
<td>Integer that indicates the value Transmit Tw_sys echoed back by the remote system. This value maps from the aLldpXdot3RemRxTwSysEcho attribute.</td>
</tr>
<tr>
<td>Remote Fallback Tw_sys (μSec)</td>
<td>Integer that indicates the value of fallback Tw_sys that the remote system is advertising. This attribute maps to the variable RemFbSystemValue as defined in 78.4.2.3.</td>
</tr>
<tr>
<td>Tx_dll_enabled</td>
<td>Initialization status of the EEE transmit Data Link Layer management function on the local system.</td>
</tr>
<tr>
<td>Tx_dll_ready</td>
<td>Data Link Layer ready: This variable indicates that the tx system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.</td>
</tr>
<tr>
<td>Rx_dll_enabled</td>
<td>Status of the EEE capability negotiation on the local system.</td>
</tr>
<tr>
<td>Rx_dll_ready</td>
<td>Data Link Layer ready: This variable indicates that the rx system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.</td>
</tr>
<tr>
<td>Power Saving (%)</td>
<td>Percentage of Power saved by enabling EEE on the interface since EEE counters are last cleared.</td>
</tr>
</tbody>
</table>
Example

console#show green-mode gi1/0/1
Energy Detect Admin Mode............ Enabled
Operational Status.................. Active
Reason................................ No Energy Detected

Short Reach Feature............... Not Available

EEE Admin Mode.................. Enabled
Rx Low Power Idle Event Count..... 0
Rx Low Power Idle Duration (uSec) 0
Tx Low Power Idle Event Count.... 0
Tx Low Power Idle Duration (uSec) 0
Tw_sys_tx (usec)....................17
Tw_sys_tx Echo(usec).................17
Tw_sys_rx (usec)....................17
Tw_sys_tx Echo(usec).................17
Fallback Tw_sys (usec).............17
Remote Tw_sys_tx (usec).............21
Remote Tw_sys_tx Echo(usec)........21
Remote Tw_sys_rx (usec).............21
Remote Tw_sys_tx Echo(usec).......21
Remote fallback Tw_sys (usec)......21
Tx DLL enabled...................Yes
Tx DLL ready.....................Yes
Rx DLL enabled...................Yes
Rx DLL ready.....................Yes
Cumulative Energy Saving (W * H)..2.37
Time Since Counters Last Cleared..1 day 20 hr 47 min 34 sec

show green-mode

Use the show green-mode command to display the green-mode configuration for the whole system. The status is shown only for the modes supported on the corresponding hardware platform whether enabled or disabled.
**Syntax**
show green-mode

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command output provides the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy Detect</strong></td>
<td></td>
</tr>
<tr>
<td>Energy-detect Config</td>
<td>Energy-detect Admin mode is enabled or disabled.</td>
</tr>
<tr>
<td>Energy-detect Opr</td>
<td>Energy detect mode is currently active or inactive. The energy detect mode may be administratively enabled, but the operational status may be inactive.</td>
</tr>
<tr>
<td><strong>EEE</strong></td>
<td></td>
</tr>
<tr>
<td>EEE Config</td>
<td>EEE Admin Mode is enabled or disabled.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show green-mode
```

Current Power Consumption (mW)................. 11545
Power Saving /Stack (%)......................... 3
Cumulative Energy Saving /Stack (W * H)........ 17

Unit Green Ethernet Features Supported
----  --------------------------------------------------------------------------------------------------
1    Energy-Detect EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est

<table>
<thead>
<tr>
<th>Interface</th>
<th>Energy-Detect</th>
<th>Short-Reach-Config</th>
<th>Short-Reach</th>
<th>EEE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Opr</td>
<td>Auto Forced Opr</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/1</td>
<td>Enabled Active</td>
<td>Enabled Disabled In-Active</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled Active</td>
<td>Enabled Disabled In-Active</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>
show green-mode eee-lpi-history interface

Use the show green-mode eee-lpi-history interface command to display the interface green-mode EEE LPI history.

Syntax

show green-mode eee-lpi-history interface interface-id

- interface-id—An Ethernet interface identifier. See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

On combo ports, samples are only collected on the copper ports when enabled.

The following fields are displayed by this command.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Interval</td>
<td>Interval at which EEE LPI statistics is collected.</td>
</tr>
<tr>
<td>Total No. of Samples to Keep</td>
<td>Maximum number of samples to keep.</td>
</tr>
<tr>
<td>Percentage LPI Time per Stack</td>
<td>Percentage of total time spent in LPI mode by all ports in the stack when compared to total time since reset.</td>
</tr>
<tr>
<td>Sample No.</td>
<td>Sample index.</td>
</tr>
</tbody>
</table>
### Example

This example is on a platform capable of providing power consumption details.

```
console#show green-mode eee-lpi-history interface gi1/0/1
```

<table>
<thead>
<tr>
<th>Sample Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time since last reset.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Interval (sec)</td>
<td>30</td>
</tr>
<tr>
<td>Total No. of Samples to Keep</td>
<td>10</td>
</tr>
<tr>
<td>Percentage LPI time per stack</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample No.</th>
<th>Time Since The Sample Was Recorded</th>
<th>Percentage of Time spent in LPI mode since last sample</th>
<th>Percentage of Time spent in LPI mode since last reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>00:00:00:09</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>00:00:00:40</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>00:00:01:11</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>
GMRP Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The GARP Multicast Registration Protocol (GMRP) provides a mechanism that allows networking devices to dynamically register (and deregister) Group membership information with the MAC networking devices attached to the same segment, and for that information to be disseminated across all networking devices in the bridged LAN that support Extended Filtering Services. The operation of GMRP relies upon the services provided by the Generic Attribute Registration Protocol (GARP). GMRP is supported as described below.

The information registered, deregistered and disseminated via GMRP is in the following forms:

1. Group Membership information: This indicates that there exists one or more GMRP participants which are members of a particular Group, and carry the group MAC addresses associated with the Group.

2. Group service requirements information: This indicates that one or more GMRP participants require Forward all Groups or Forward Unregistered to be the default filtering behavior.

NOTE: The Group Service capability is not supported.

Registration of group membership information allow networking devices to be made aware that frames destined for that group MAC address concerned should be forwarded in the direction of registered members of the group. Forwarding of frames destined for that group MAC address occur on ports on which such membership registration has been received.

Registration of group services requirement information allow networking devices to be made aware that any of their ports that can forward frames in the direction from which the group service requirement information has been received should modify their default group behavior in accordance with the group service requirement expressed.

The registration and deregistration of membership results in the multicast table being updated with a new entry or the existing entry modified.
This ensures that the networking device receives multicast frames from all ports but forwards them through only those ports for which GMRP has created Group registration entry (for that multicast address). Registration entries created by GMRP ensures that frames are not transmitted on LAN segments which neither have registered GMRP participants nor are in the path through the active topology between the sources of the frames and the registered group members.

NOTE: This feature is not available on the N3000 when loaded with the AGGREGATION ROUTER enabled firmware (e.g., N3000_BGPvA.B.C.D.stk).

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmrp enable</td>
<td>Use the <code>gmrp enable</code> command in Global Configuration mode to enable GMRP globally or Interface Configuration mode to enable GMRP on a port.</td>
</tr>
<tr>
<td>show gmrp configuration</td>
<td></td>
</tr>
<tr>
<td>clear gmrp statistics</td>
<td></td>
</tr>
<tr>
<td>–</td>
<td></td>
</tr>
</tbody>
</table>

### gmrp enable

Use the `gmrp enable` command in Global Configuration mode to enable GMRP globally or Interface Configuration mode to enable GMRP on a port.

**Syntax**

- `gmrp enable`
- `no gmrp enable`

**Default Configuration**

GMRP is disabled by default.

**Command Mode**

Global Configuration and Interface Configuration modes

**User Guidelines**

IGMP snooping is incompatible with GMRP and must be disabled on any VLANs running GMRP.
Example
In this example, GMRP is globally enabled.

console(config)#gmrp enable

clear gmrp statistics

Use the clear gmrp statistics command to clear all the GMRO statistics information.

Syntax

clear gmrp statistics [{gigabitethernet unit/slot/port | port-channel port-
channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet
unit/slot/port}]

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
The following example clears all the GMRP statistics information on port
Gi1/0/8.

console# clear gmrp statistics gigabitethernet 1/0/8

show gmrp configuration

Use the show gmrp configuration command in Global Configuration mode
and Interface Configuration mode to display GMRP configuration.

Syntax

show gmrp configuration
Default Configuration
GMRP is disabled by default.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
console#show gmrp configuration

Global GVRP Mode: Disabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Join Timer (centisecs)</th>
<th>Leave Timer (centisecs)</th>
<th>LeaveAll Timer (centisecs)</th>
<th>GVRP Mode</th>
<th>Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>20</td>
<td>90</td>
<td>1000</td>
<td>Enabled</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/13</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/15</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/16</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/17</td>
<td>20</td>
<td>60</td>
<td>1000</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GVRP Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

GARP VLAN Registration Protocol (GVRP) is used to propagate VLAN membership information throughout the network. GVRP is based on the Generic Attribute Registration Protocol (GARP), which defines a method of propagating a defined attribute (that is, VLAN membership) throughout the network. GVRP allows both end stations and the networking device to issue and revoke declarations relating to membership in VLANs. End stations that participate in GVRP register VLAN membership using GARP Protocol Data Unit (GPDU) messages. Networking devices that implement the GVRP protocol and enable GVRP then process the GPDUs. The VLAN registration is made in the context of the port that receives the GPDU. The networking device propagates this VLAN membership on all of its other ports in the active topology. Thus, the end station VLAN ID is propagated throughout the network. GVRP is an application defined in the IEEE 802.1p standard that allows for the control of 802.1Q VLANs.

NOTE: This feature is not available on the N3000 when loaded with the AGGREGATION ROUTER enabled firmware (e.g., N3000_BGPvA.B.C.D.stk).

Commands in this Section

This section explains the following commands:

- clear gvrp statistics
- garp timer
- gvrp enable (Global Configuration)
- gvrp enable (Interface Configuration)
- gvrp registration-forbid
- gvrp vlan-creation-forbid
- show gvrp configuration
- show gvrp error-statistics
- show gvrp statistics
- –

**clear gvrp statistics**

Use the clear gvrp statistics command to clear all the GVRP statistics information.
**Syntax**
clear gvrp statistics [interface-id]
  •  interface-id—An Ethernet interface identifier or a port channel identifier

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example clears all the GVRP statistics information on interface Gi1/0/8.

```
console# clear gvrp statistics gigabitethernet 1/0/8
```

**garp timer**
Use the `garp timer` command in Interface Configuration mode to adjust the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the `no` form of this command.

**Syntax**
garp timer {join | leave | leaveall} timer_value
no garp timer
  •  join — Indicates the time in centisseconds that PDUs are transmitted.
  •  leave — Indicates the time in centiseconds that the device waits before leaving its GARP state.
  •  leaveall — Used to confirm the port within the VLAN. The time is the interval between messages sent, measured in centiseconds.
  •  timer_value — Timer values in centiseconds. The range is 10-100 for `join`, 20-600 for `leave`, and 200-6000 for `leaveall`.  
Default Configuration

The default timer values are as follows:

- Join timer — 20 centiseconds
- Leave timer — 60 centiseconds
- Leaveall timer — 1000 centiseconds

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command is available in Ethernet interface configuration mode and port channel interface configuration mode. The following relationships for the various timer values must be maintained:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

The timer_value setting must be a multiple of 10.

Example

The following example sets the leave timer for port 1/0/8 to 90 centiseconds.

```
console (config)# interface gigabitethernet 1/0/8
console (config-if-Gi1/0/8)# garp timer leave 90
```

**gvrp enable (Global Configuration)**

Use the `gvrp enable (global)` command in Global Configuration mode to enable GVRP globally on the switch. To disable GVRP globally on the switch, use the `no` form of this command.

**Syntax**

`gvrp enable`
no gvrp enable

**Default Configuration**
GVRP is globally disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example globally enables GVRP on the device.
```
console(config)#gvrp enable
```

**gvrp enable (Interface Configuration)**
Use the `gvrp enable` command in Interface Configuration mode to enable GVRP on an interface. To disable GVRP on an interface, use the `no` form of this command.

**Syntax**
gvrp enable
no gvrp enable

**Default Configuration**
GVRP is disabled on all interfaces by default.

**Command Mode**
Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode
**User Guidelines**

This command is available in Ethernet interface configuration mode and port channel interface configuration mode. An Access port cannot join dynamically to a VLAN because it is always a member of only one VLAN. Membership in untagged VLAN would be propagated in a same way as a tagged VLAN. In such cases it is the administrator’s responsibility to set the PVID to be the untagged VLAN VID.

**Example**

The following example enables GVRP on Gigabit Ethernet 1/0/8.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#gvrp enable
```

**gvrp registration-forbid**

Use the `gvrp registration-forbid` command in Interface Configuration mode to deregister all VLANs on a port and prevent any dynamic registration on the port. To allow dynamic registering for VLANs on a port, use the no form of this command.

**Syntax**

```
gvrp registration-forbid
no gvrp registration-forbid
```

**Default Configuration**

Dynamic registering and deregistering for each VLAN on the port is not forbidden.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command is available in Ethernet interface configuration mode and port channel interface configuration mode.
Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port 1/0/8.

```bash
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#gvrp registration-forbid
```

**gvrp vlan-creation-forbid**

Use the `gvrp vlan-creation-forbid` command in Interface Configuration mode to disable dynamic VLAN creation. To enable dynamic VLAN creation, use the `no` form of this command.

**Syntax**

- `gvrp vlan-creation-forbid`
- `no gvrp vlan-creation-forbid`

**Default Configuration**

By default, dynamic VLAN creation is enabled.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command is available in Ethernet interface configuration mode and port channel interface configuration mode.

**Example**

The following example disables dynamic VLAN creation on port 1/0/8.

```bash
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#gvrp vlan-creation-forbid
```
show gvrp configuration

Use the show gvrp configuration command to display GVRP configuration information. Timer values are displayed. Other data shows whether GVRP is enabled and which ports are running GVRP.

Syntax

show gvrp configuration [ interface-id ]

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command is valid for Ethernet and port-channel interfaces. If no interface-id parameter is given, all interfaces are shown.

Example

The following example shows how to display GVRP configuration information:

```
console# show gvrp configuration
Global GVRP Mode: Disabled
Join                  Leave                LeaveAll               Port      VLAN
Interface      Timer (centisecs) Timer (centisecs) Timer (centisecs) GVRP Mode Create Register Forbid Forbid
-----------  -----------  -----------  -----------  ----------- ------ -------- -------- -------- -------- -------- -------- --------</---- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- -------- ----
show gvrp error-statistics

Use the show gvrp error-statistics command in User Exec mode to display GVRP error statistics.

Syntax

show gvrp error-statistics [interface-id]

- interface-id—An Ethernet interface identifier or a port channel interface identifier.

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

If no interface-id parameter is given, all interfaces are shown.

Example

The following example displays GVRP error statistics information.

    console>show gvrp error-statistics

GVRP error statistics:
----------------------
Legend:

INVPROT: Invalid Protocol Id  INVATYP: Invalid Attribute Type
INVALEN: Invalid Attribute Length INVAVAL: Invalid Attribute Value
INVEVENT: Invalid Event

<table>
<thead>
<tr>
<th>Port</th>
<th>INVPROT</th>
<th>INVATYP</th>
<th>INVALEN</th>
<th>INVAVAL</th>
<th>INVEVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
</tbody>
</table>
show gvrp statistics

Use the `show gvrp statistics` command in User Exec mode to display GVRP statistics.

**Syntax**

`show gvrp statistics [interface-id]`

- **interface-id** — An Ethernet interface identifier or a port channel interface identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

This example shows output of the `show gvrp statistics` command.

```console
console>show gvrp statistics

GVRP statistics:
------------------------
Legend:

rJE  : Join Empty Received         rJIn : Join In Received
rEmp : Empty Received              rLIn : Leave In Received
rLE  : Leave Empty Received        rLA  : Leave All Received
sJE  : Join Empty Sent             JIn  : Join In Sent
sEmp : Empty Sent                  sLIn : Leave In Sent
sLE  : Leave Empty Sent            sLA  : Leave All Sent
```
<table>
<thead>
<tr>
<th>Port</th>
<th>rJE</th>
<th>rJIn</th>
<th>rEmp</th>
<th>rLIn</th>
<th>rLE</th>
<th>rLA</th>
<th>sJE</th>
<th>sJIn</th>
<th>sEmp</th>
<th>sLIn</th>
<th>sLE</th>
<th>sLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Snooping of Internet Group Management Protocol (IGMP) messages is a feature that allows Dell EMC Networking switches to forward multicast traffic intelligently on the switch. Multicast traffic is traffic that is destined to a host group. Host groups are identified by the destination MAC address, i.e. the range 01:00:5e:00:00:00-01:00:5e:7f:ff:ff for IPv4 multicast traffic or 33:33:xx:xx:xx:xx for IPv6 multicast traffic. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP snooping switches build forwarding lists by monitoring for, and in some cases intercepting, IGMP messages. Although the software processing the IGMP messages could maintain state information based on the full IP group addresses, the forwarding tables in Dell EMC Networking are mapped to link layer addresses.

The Multicast Forwarding Database (MFDB) manages the forwarding address table for Layer 2 multicast protocols, such as IGMP Snooping.

The IGMP Snooping code in the CPU ages out IGMP entries in the MFDB. If a report for a particular group on a particular interface is not received within a certain time interval (query interval), the IGMP Snooping code deletes that interface from the group. The value for query interval time is configurable using management.

If an IGMP Leave Group message is received on an interface, the IGMP Snooping code sends a query on that interface and waits a specified length of time (maximum response time). If no response is received within that time, that interface is removed from the group. The value for maximum response time is configurable using management.

In addition to building and maintaining lists of multicast group memberships, the snooping switch also maintains a list of multicast routers. When forwarding multicast packets, they should be forwarded on ports that have joined using IGMP and also on ports on which multicast routers are attached. The reason for this is that in IGMP there is only one active query mechanism. This means that all other routers on the network are suppressed.
and thus not detectable by the switch. If a query is not received on an interface within a specified length of time (multicast router present expiration time), that interface is removed from the list of interfaces with multicast routers attached. The multicast router present expiration time is configurable using management. The default value for the multicast router expiration time is zero, which indicates an infinite time-out (that is, no expiration).

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>ip igmp snooping vlan groupmembership-interval</td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>ip igmp snooping vlan last-member-query-interval</td>
</tr>
<tr>
<td>show ip igmp snooping groups</td>
<td>ip igmp snooping vlan mrouter</td>
</tr>
<tr>
<td>show ip igmp snooping mrouter</td>
<td>ip igmp snooping report-suppression</td>
</tr>
<tr>
<td>ip igmp snooping vlan immediate-leave</td>
<td>ip igmp snooping unregistered floodall</td>
</tr>
<tr>
<td>--</td>
<td>ip igmp snooping vlan mrouter</td>
</tr>
</tbody>
</table>

**ip igmp snooping**

Use the `ip igmp snooping` command in Global Configuration mode without parameters to globally enable Internet Group Management Protocol (IGMP) snooping. Use the `vlan` form of the command to enable IGMP snooping on a specific VLAN. Use the `no` form of this command to disable IGMP snooping globally.

**Syntax**

```
ip igmp snooping [vlan vlan-id]
no ip igmp snooping [vlan vlan-id]
```

- `vlan-id`—Specifies a VLAN ID value.
Default Configuration
IGMP snooping is enabled globally and on all VLANs by default.

Command Mode
Global Configuration mode

User Guidelines
Use this command without parameters to globally enable IGMP snooping. Use the no form of the command to disable IGMP snooping. Use the vlan parameter to enable IGMP snooping on a specific VLAN. GMRP is incompatible with IGMP snooping and should be disabled on any VLANs on which IGMP snooping is enabled. It is recommended that MLD snooping should be enabled whenever IGMP snooping is enabled to ensure that unwanted pruning of multicast protocol packets used by other protocols does not occur.

Enabling IGMP snooping on a VLAN in which L3 multicast is enabled is recommended. If a multicast source is connected to a VLAN on which both L3 multicast and IGMP/MLD snooping are enabled, the multicast source is forwarded to the mrouter ports, including the internal mrouter port. If IGMP snooping is disabled, multicast data plane packets are flooded in the VLAN.

IGMP snooping (and IGMP querier) validates IGMP packets. As part of the validation, IGMP checks for the router alert option. If other devices in the network do not send IGMP packets with the router alert option, IGMP snooping (and snooping querier) will discard the packet. Use the no ip igmp snooping router-alert-check command to disable checking for the router alert option. IGMP packets are intended to be confined to the local link, IGMP snooping validates that the IP TTL is 1 and discards packets with other values.

Example
console(config)#ip igmp snooping
console(config)#no ip igmp snooping vlan 1

Command History
Revised in 6.3.5 release.
show ip igmp snooping

Use the show ip igmp snooping command to display the IGMP snooping configuration and SSM statistics.

**Syntax**

show ip igmp snooping [vlan vlan-id]

- vlan-id—Specifies a VLAN ID value.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config)#show ip igmp snooping

Admin Mode................................. Enable
IGMP Router-Alert check.................... Enabled
Multicast Control Frame Count.............. 0
SSM FDB Capacity.......................... 0
SSM FDB Current Entries................... 0
SSM FDB High Water Mark. ................ 0
Flooding Unregistered to All Ports......... Disabled

Vlan 1:
--------
IGMP Snooping Admin Mode.................. Enabled
Immediate Leave Mode...................... Disabled
Group Membership Interval................ 260
Last Member Query Interval................. 10
Multicast Router Expiry Time.............. 300
Report Suppression Mode................... Enabled
```
show ip igmp snooping groups

Use the show ip igmp snooping groups command in User Exec mode to display the multicast groups learned by IGMP snooping and IGMP SSM entries.

Syntax

show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address]

- vlan-id — Specifies a VLAN ID value.
- ip-multicast-address — Specifies an IP multicast address.

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

To see the full multicast address table (including static addresses) use the show mac address-table command.

Example

This example shows IGMPv2 snooping entries

console(config)#show ip igmp snooping groups

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Type</th>
<th>OIFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.129</td>
<td>Dynamic</td>
<td>Te1/0/1,Te1/0/17</td>
</tr>
</tbody>
</table>

IGMP SSM Entries:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Group</th>
<th>Reporter</th>
<th>Filter</th>
<th>IIF</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224.2.2.2</td>
<td>192.168.10.2</td>
<td>include</td>
<td>Te1/0/1</td>
<td>1.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.2.2.2</td>
</tr>
</tbody>
</table>
Layer 2 Switching Commands

1 224.3.3.3  192.168.10.2  include Te1/0/1  4.4.4.4

VLAN Group  Reporter  Filter  IIF  Source Address
-------  -----------------  -------  ------  --------------
1  224.2.2.2  192.168.10.2  include Te1/0/1  1.1.1.2

console(config)#show ip igmp snooping

Admin Mode..................................... Enable
IGMP Router-Alert check........................ Disabled
Multicast Control Frame Count............... 6847
SSM FDB Capacity............................... 128
SSM FDB High Water Mark..................... 1
SSM FDB Current Entries..................... 1
Flooding Unregistered to All Ports........... Disabled

Vlan 1:
-------
IGMP Snooping Admin Mode..................... Enabled
Immediate Leave Mode.......................... Disabled
Group Membership Interval................... 260
Last Member Query Interval.................. 10
Multicast Router Expiry Time............... 300
Report Suppression Mode........................ Enabled

**show ip igmp snooping mrouter**

Use the **show ip igmp snooping mrouter** command to display information on dynamically learned multicast router interfaces.

**Syntax**

show ip igmp snooping mrouter

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
The following example shows IGMP snooping mrouter information.

```
crash#show ip igmp snooping mrouter
VLAN ID   Port
-------   -----------
10        Gi2/0/1
```

**ip igmp snooping vlan immediate-leave**
This command enables or disables IGMP Snooping immediate-leave mode on a selected VLAN.

**Syntax**
```
ip igmp snooping vlan vlan-id immediate-leave
no ip igmp snooping vlan vlan-id immediate-leave
```
- vlan id — A VLAN identifier (range 1-4093).

**Default Configuration**
IGMP snooping immediate-leave mode is disabled on VLANs by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
Enabling immediate-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. The no form of this command disables IGMP Snooping immediate-leave mode on a VLAN.

Enable immediate-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This setting prevents the inadvertent dropping of the other hosts that were connected to the same Layer 2 LAN.
port, but were still interested in receiving multicast traffic directed to that group. Also, immediate-leave processing is supported only with IGMP version 2 hosts.

**Example**
The following example enables IGMP snooping immediate-leave mode on VLAN 2.

```
console(config)#ip igmp snooping vlan 2 immediate-leave
```

**ip igmp snooping vlan groupmembership-interval**

This command sets the IGMP Group Membership Interval time on a VLAN.

**Syntax**

```
ip igmp snooping vlan vlan-id groupmembership-interval time
no ip igmp snooping vlan vlan-id groupmembership-interval
```

- **vlan-id** — A VLAN identifier (Range 1-4093).
- **time** — IGMP group membership interval time in seconds. (Range: 2–3600)

**Default Configuration**

The default group membership interval time is 260 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds. The **no** form of this command sets the IGMPv3 Group Membership Interval time to the default value.
**Example**
The following example configures an IGMP snooping group membership interval of 1500 seconds on VLAN 2.

```console
console(config)#ip igmp snooping vlan 2 groupmembership-interval 1500
```

**ip igmp snooping vlan last-member-query-interval**

This command sets the last-member-query interval on a particular VLAN.

**Syntax**

- `ip igmp snooping vlan vlan-id last-member-query-interval time`
- `no ip igmp snooping vlan vlan-id last-member-query-interval`

- **vlan-id** — A VLAN identifier (Range 1-4093).
- **time** — Number of seconds after which a host is considered to have left the group. (Range: 1-25)

**Default Configuration**
The default maximum response time is 10 seconds.

**Command Mode**
Global Configuration mode

**User Guidelines**
The last-member-query-interval is the amount of time in seconds after which a host is considered to have left the group. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds. The `no` form of this command sets the last-member-query-interval on the VLAN to the default value. When using IGMP Snooping Querier, this parameter should be less than the value for the IGMP Snooping Querier query interval.

**Example**
The following example sets the maximum response time to 7 seconds on VLAN 2.

```console
console(config)#ip igmp snooping vlan 2 last-member-query-interval 7
```
ip igmp snooping vlan mcrtexpiretime

This command sets the multicast router present expiration time. The time is set on a particular VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 1–2147483647 seconds. A value of 0 indicates an infinite time-out (no expiration). The no form of this command sets the multicast router present expiration time to 0.

Syntax

ip igmp snooping vlan vlan-id mcrtexpiretime time
no ip igmp snooping vlan vlan-id mcrtexpiretime

• vlan-id — A VLAN identifier (Range 1-4093).
• time— Multicast router present expiration time. (Range: 1–3600)

Default Configuration

The default multicast router present expiration time is 300 seconds.

Command Mode

Global Configuration mode

User Guidelines

The expiry time is configured for an individual VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 1–2147483647 seconds. A value of 0 indicates an infinite time-out (no expiration). The no form of this command sets the multicast router present expiration time to 0. The mcrtexpiretime should be less than the group membership interval.

Example

The following example sets the multicast router present expiration time on VLAN 2 to 60 seconds.

console(config)#ip igmp snooping vlan 2 mcrtexpiretime 1500
**ip igmp snooping report-suppression**

This command enables IGMP report suppression on a specific VLAN. The **no** form of this command disables report suppression.

**Syntax**

```
ip igmp snooping vlan vlan-id report-suppression
no ip igmp snooping vlan vlan-id report-suppression
```

- **vlan-id** — A VLAN identifier (Range 1-4093).

**Default Configuration**

Report suppression is enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

When IGMP report suppression is enabled, the switch only sends the first report received for a group in response to a query. Report suppression is only applicable to IGMPv1 and IGMPv2.

**Example**

The following example sets the snooping report suppressions time to 10 seconds.

```
console(config)#ip igmp snooping vlan 10 report-suppression
```

**ip igmp snooping unregistered floodall**

This command enables flooding of unregistered multicast traffic to all ports in the VLAN. Use the **no** form of this command to only flood unregistered multicast traffic to multicast router ports.

**Syntax**

```
ip igmp snooping unregistered floodall
no ip igmp snooping unregistered floodall
```
**Default Configuration**

Unregistered multicast traffic is only flooded to router ports by default. If no mrouter ports are configured, or IGMP snooping cannot identify a multicast router, then unregistered multicast is flooded to all ports in the VLAN.

**Command Mode**

Global Configuration mode.

**User Guidelines**

There is no equivalent MLD command since this setting applies to both protocols.

**Example**

```
console(config)#ip igmp snooping unregistered floodall
```

**ip igmp snooping vlan mrouter**

This command statically configures a port as connected to a multicast router for a specified VLAN. Use the no form of this command to remove the static binding.

**Syntax**

```
ip igmp snooping vlan vlan-id mrouter interface interface-id
no ip igmp snooping vlan vlan-id mrouter interface interface-id
```

- **vlan-id** — A VLAN identifier (Range 1-4093).
- **interface-id** — The next-hop interface to the multicast router. Ethernet interface identifiers and port channel identifiers are allowed.

**Default Configuration**

There are no multicast router ports configured by default.

**Command Mode**

Global Configuration mode.
User Guidelines

It is preferable to configure mrouter ports for IGMP snooping as opposed to configuring a static MAC address entry for the router. A static MAC address entry is tied to a specific port whereas an mrouter configuration will dynamically learn the MAC address of the router. Multiple mrouter ports may be configured for a VLAN.

IGMP snooping will consider that an mrouter is active if an mrouter port is defined in the VLAN, regardless of whether the mrouter port is up or not. If an mrouter port is defined, IGMP snooping will not flood unregistered multicast packets received in the VLAN. This behavior can be used to ensure that IGMP snooping will selectively forward IPv4 multicast data traffic in a VLAN even if no dynamically discovered IPv4 multicast router has been discovered.

Multicast data plane traffic from multicast sources in a VLAN is always forwarded to the mrouter ports in the VLAN. Multicast control plane packets (those addressed to the reserved 224.0.0.X address) are always flooded to all ports in the VLAN, regardless of whether an mrouter port is defined or not.

Example

```
console(config)#ip igmp snooping vlan 10 mrouter interface Gi1/0/2
```
The IGMP Snooping Querier is an extension to the IGMP Snooping feature. IGMP Snooping Querier allows the switch to simulate an IGMP router in a Layer 2-only network, thus removing the need to have an IGMP Router to collect and refresh the multicast group membership information. The querier function simulates a small subset of the IGMP router functionality. IGMP Snooping Querier is not recommended for networks in which a multicast router is reachable.

In a network with IP multicast routing, an IP multicast router acts as the IGMP querier. However, if it is required that the IP-multicast traffic in a VLAN be switched and no multicast router is present in the network, the Dell EMC Networking switch can be configured as an IGMP querier. When IGMP Snooping Querier is enabled, the Querier sends out periodic IGMP General Queries that trigger the multicast listeners/members to send their joins to the querier so as to receive the multicast data traffic. IGMP snooping listens to these reports to establish the appropriate L2 forwarding table entries.

The Dell EMC Networking supports version IGMP V1 and 2 for snooping IGMP queries.

Commands in this Section

This section explains the following commands:

- **ip igmp snooping querier**
- **ip igmp snooping querier timer expiry**
- **ip igmp snooping querier election participate**
- **ip igmp snooping querier version**
- **ip igmp snooping querier query-interval**
- **show ip igmp snooping querier**

**ip igmp snooping querier**

This command enables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN.
Syntax

ip igmp snooping querier [vlan vlan-id] [address ip-address]

no ip igmp snooping querier [vlan vlan-id][address]

- vlan-id — A valid VLAN number.
- ip-address — An IPv4 address used for the source address.

Default Configuration

The IGMP Snooping Querier feature is globally disabled on the switch. When enabled, the IGMP Snooping Querier stops sending queries if it detects IGMP queries from a multicast-enabled router. The Snooping Querier periodically (querier timer expiry) wakes up and listens for IGMP queries, and if found, goes back to sleep. If no IGMP queries are heard, then the Snooping Querier will resume querying.

Command Mode

Global Configuration mode

User Guidelines

Using this command, you can specify the IP address that the snooping querier switch should use as the source address when generating periodic queries. The no form of this command disables IGMP Snooping Querier on the system. Use the optional address parameter to set or reset the querier address.

If a VLAN has IGMP Snooping Querier enabled, and IGMP Snooping is operationally disabled on the VLAN, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping Querier functionality is reenabled if IGMP Snooping becomes operational on the VLAN. The IGMP Snooping Querier application sends periodic general queries on the VLAN to solicit membership reports.

When using the command in Global Configuration mode to configure a snooping querier source address, the IPv4 address is the global querier address. When using the command in VLAN Configuration mode to configure a snooping querier source address, the IPv4 address is the querier address for the VLAN. If there are no global or VLAN querier addresses configured, then the management IP address is used as the IGMP snooping querier source address. Using all zeros for the querier IP address disables it.
The VLAN IP address takes precedence over the global IP address when both are configured. IGMP Querier does not detect when the local switch is configured as a multicast router. It is not recommended to configure both L3 multicast routing and IGMP Querier on the same switch.

IGMP snooping (and IGMP querier) validates IGMP packets. As part of the validation, IGMP checks for the router alert option. If other devices in the network do not send IGMP packets with the router alert option, IGMP snooping (and snooping querier) will discard the packet. Use the `no ip igmp snooping router-alert-check` command to disable checking for the router alert option.

**Example**

The following example enables IGMP snooping querier in Global Configuration mode.

```console
console(config)#ip igmp snooping querier vlan 1 address 10.19.67.1
ip igmp snooping querier election participate
```

**ip igmp snooping querier election participate**

This command enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Snooping Querier in the VLAN.

**Syntax**

```
ip igmp snooping querier election participate vlan-id
no ip igmp snooping querier election participate vlan-id
```

**Parameters**

- `vlan-id`—The VLAN identifier on which the querier is expected to operate. Range 1-4093.

**Default Configuration**

The snooping querier is configured to not participate in the querier election by default.

**Command Mode**

Global Configuration mode
User Guidelines

When election mode is enabled, if the Snooping Querier finds that the other Querier source address is numerically higher than the Snooping Querier address, it stops sending periodic queries. The Snooping Querier with the numerically lower IP address wins the election, and continues sending periodic queries. The no form of this command sets the snooping querier not to participate in the querier election but to stop sending queries as soon as it discovers the presence of another querier in the VLAN. If the switch detects another querier in the VLAN, it will cease sending queries for the querier timeout period.

Example

The following example configures the snooping querier to participate in the querier election on VLAN 10.

```
console(config)#ip igmp snooping querier election participate 10
```

ip igmp snooping querier query-interval

This command sets the IGMP Querier Query Interval time, which is the amount of time in seconds that the switch waits before sending another periodic query. The no form of this command sets the IGMP Querier Query Interval time to its default value.

Syntax

```
ip igmp snooping querier query-interval interval-count
no ip igmp snooping querier query-interval
```

- interval-count — Amount of time in seconds that the switch waits before sending another general query. (Range: 1-1800)

Default Configuration

The query interval default is 60 seconds.

Command Mode

Global Configuration mode
User Guidelines

The value of this parameter should be larger than the IGMP Max Response Time value inserted into general query messages by the querier. The default IGMP Max Response Time is defined in RFC 3376 as 10 seconds. Dell EMC Networking queriers use this value when sending general query messages.

Use the show ip igmp snooping querier vlan command to display the operational max response time value.

Example

The following example sets the query interval to 1800:

```
console(config)#ip igmp snooping querier query-interval 1800
```

ip igmp snooping querier timer expiry

This command sets the IGMP querier timer expiration period which is the time period that the switch remains in non-querier mode after it has discovered that there is a multicast querier in the network. The no form of this command sets the IGMP querier timer expiration period to its default value.

Syntax

```
ip igmp snooping querier timer expiry seconds
no ip igmp snooping querier timer expiry
```

- **seconds** — The time in seconds that the switch remains in Non-Querier mode after it has discovered that there is a multicast querier in the network. The range is 60–300 seconds.

Default Configuration

The query interval default is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.
**Example**
The following example sets the querier timer expiry time to 100 seconds.

```
console(config)#ip igmp snooping querier timer expiry 100
```

**ip igmp snooping querier version**
This command sets the IGMP version of the query that the snooping switch is going to send periodically. The no form of this command sets the IGMP Querier Version to its default value.

**Syntax**

```
ip igmp snooping querier version version
no ip igmp snooping querier version
```

- **version** — IGMP version. (Range: 1–2)

**Default Configuration**
The querier version default is 2.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets the IGMP version of the querier to 1.

```
console(config)#ip igmp snooping querier version 1
```

**show ip igmp snooping querier**
This command displays IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled. If a querier is active in the network and IGMP snooping querier is enabled, the querier’s IP address is shown in the Last Querier Address field.
**Syntax**

show ip igmp snooping querier [detail | vlan vlan-id]

- vlan-id — Specifies a VLAN ID value.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all submodes

**User Guidelines**

When the optional argument vlan-id is not used, the command shows the following information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping Querier</td>
<td>Indicates whether or not IGMP Snooping Querier is active on the switch.</td>
</tr>
<tr>
<td>IGMP Version</td>
<td>Indicates the version of IGMP that will be used while sending out the queries.</td>
</tr>
<tr>
<td>Querier Address</td>
<td>Shows the IP address that is used in the IPv4 header when sending out IGMP queries. It can be configured using the appropriate command.</td>
</tr>
<tr>
<td>Querier Query Interval</td>
<td>Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.</td>
</tr>
<tr>
<td>Querier Expiry Interval</td>
<td>Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.</td>
</tr>
</tbody>
</table>

When a value is given for vlan-id, the following information appears.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping Querier VLAN Mode</td>
<td>Indicates whether IGMP Snooping Querier is active on the VLAN.</td>
</tr>
</tbody>
</table>
Layer 2 Switching Commands

If no querier has been elected, the Elected Querier output is not shown. If the querier has not received any queries, then the Last Querier Address information is not shown. When the optional argument detail is used, the command shows the global information and the information for all Querier enabled VLANs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational State</td>
<td>Indicates whether IGMP Snooping Querier is in the Querier or Non-Querier state. When the switch is in Querier state it sends out periodic general queries. When in Non-Querier state it waits for moving to Querier state and does not send out any queries.</td>
</tr>
<tr>
<td>VLAN Operational Max Response Time</td>
<td>Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.</td>
</tr>
<tr>
<td>Querier Election Participate Mode</td>
<td>Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.</td>
</tr>
<tr>
<td>Last Address</td>
<td>Indicates the IP address of the most recent Querier from which a Query was received.</td>
</tr>
<tr>
<td>Operational Version</td>
<td>Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.</td>
</tr>
<tr>
<td>Elected Querier</td>
<td>Indicates the IP address of the Querier that has been designated as the Querier based on its source IP address. This field will be 0.0.0.0 when Querier Election Participate mode is disabled.</td>
</tr>
</tbody>
</table>

If no querier has been elected, the Elected Querier output is not shown. If the querier has not received any queries, then the Last Querier Address information is not shown. When the optional argument detail is used, the command shows the global information and the information for all Querier enabled VLANs.

**Example**

The following example shows querier information for VLAN 1.

```console
console#show ip igmp snooping querier vlan 1

Vlan 1 : IGMP Snooping querier status

-----------------------------------------------
IGMP Snooping Querier Vlan Mode.............. Enable
Querier Election Participate Mode............ Disable
Querier Vlan Address........................... 10.19.67.1
```

Layer 2 Switching Commands | 497
Operational State........................... Querier
Operational version........................ 1
Interface Error Disable and Auto Recovery

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Interface error disable automatically disables an interface when an error is detected; no traffic is allowed until the interface is either manually re-enabled or, if auto recovery is configured, the configured auto recovery time interval has passed.

For interface error disable and auto recovery, when an error condition is detected for an interface, the interface is placed in a diagnostic disabled state by shutting down the interface. The error disabled interface does not allow any traffic until the interface is re-enabled. The error disabled interface can be manually enabled using the no shutdown command. Alternatively administrator can enable auto recovery feature. Dell EMC Networking Auto Recovery re-enables the interface after the expiry of configured time interval.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errdisable recovery cause</code></td>
<td>show errdisable recovery</td>
</tr>
<tr>
<td><code>errdisable recovery interval</code></td>
<td>show interfaces status err-disabled</td>
</tr>
</tbody>
</table>

errdisable recovery cause

Use the errdisable recovery cause command to enable automatic recovery of any interface when disabled from the listed cause. Use the no form of the command to disable auto-recovery globally or for a specific cause.

Syntax

```
errdisable recovery cause {all | arp-inspection | bpduguard | bcast-storm | bpdustorm | denial-of-service | dhcp-rate-limit | loop-protect | mcast-storm | port-security | sfp-mismatch | sfpplus-mismatch | spanning-tree | udld | ucast-storm}
```
• All — Recovery for all possible causes is enabled.
• bpduguard — BPDU Guard auto-recovery.
• bcast-storm — Broadcast storm auto-recovery.
• bpdustorm — BPDU Storm auto-recovery.
• denial-of-service — Denial of Service auto-recovery.
• loop-protect — Loop Protection auto-recovery.
• port-security — Port security MAC locking auto-recovery.
• mcast-storm — Multicast Storm auto-recovery.
• sfp-mismatch — SFP mismatch auto-recovery.
• sfpplus-mismatch — SFP+ transceiver inserted in SFP port auto-recovery.
• spanning-tree — Spanning-tree auto-recovery.
• udld — UDLD auto-recovery.
• ucast-storm — Unicast Storm auto-recovery.

Default Configuration
No recovery causes are enabled by default.

Command Mode
Global Configuration mode

User Guidelines
Error disabled interfaces indicate that a problem occurred that must be resolved by the administrator. This could be a configuration problem or a physical problem (wiring) and does not necessarily indicate a problem with the switch.

This command enables auto-recovery of an interface for the specified cause (e.g., bpduguard) or all causes. An interface in the disabled state due to the configured cause is recovered (link up) when the recovery interval expires. If the interface continues to encounter errors (from any listed cause), it may be placed back in the diag-disable state and the interface will be disabled (link down).

Interfaces in the disabled state due to a listed cause may be manually recovered by entering the no shutdown command for the interface.
Interfaces in the disabled state may be manually shut down. These interfaces will not be recovered.

Auto-recovery applies to Ethernet interfaces and link aggregation groups.

**Command History**

Implemented in version 6.3.0.1 firmware. Additional causes added in version 6.5 firmware.

**Example**

The following example enables auto-recovery for all causes.

```
console(config)#errdisable recovery cause all
```

**errdisable recovery interval**

Use the `errdisable recovery interval` command to configure the interval for error recovery of interfaces disabled due to any cause. Use the `no` form of the command to reset the interval to the default.

**Syntax**

```
errdisable recovery interval interval
```

- `interval` — The interval in seconds. The range is 30-3600 seconds. The default is 300 seconds.

**Default Configuration**

The default interval is 300 seconds. Range 30-3600 seconds.

No recovery causes are enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Error disabled interfaces indicate that a problem that must be resolved by the administrator. This could be a configuration problem or a physical problem and does not necessarily indicate a problem with the switch.
When the interval expires, the system examines the error disabled interfaces and recovers them if recovery for the indicated cause is enabled. Only a single timer is used and recovery occurs when the timer expires, not when the interface time expires.

Interfaces recovered by auto-recovery issue a log message indicating that recovery is being attempted.

```
<13> Sep 25 14:38:32 10.130.135.107-1 UDLD[nim_t]: udld_util.c(1829) 87 %% Interface Gi1/0/1 is restored from the error disabled state.
```

**Command History**

Implemented in version 6.3.0.1 firmware.

**Example**

The following example sets the error recovery timer to 30 seconds.

```
console(config)#errdisable recovery interval 30
```

**show errdisable recovery**

Use the `show errdisable recovery` command to display the error disable configuration for each possible cause.

**Syntax**

```
show errdisable recovery
```

**Default Configuration**

By default, no recovery causes are enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Error disabled interfaces indicate that a problem that must be resolved by the administrator. This could be a configuration problem or a physical problem and does not necessarily indicate a problem with the switch.
When the interval expires, the system examines the error disabled interfaces and recovers them if recovery for the indicated cause is enabled. Only a single timer is used and recovery occurs when the timer expires, not when the interface time expires.

Interfaces recovered by auto-recovery issue a log message indicating that recovery is being attempted.

<13> Sep 25 14:38:32 10.130.135.107-1 UDLD[nim_t]: udld_util.c(1829) 87 %% Interface Gi1/0/1 is restored from the error disabled state.

The following information is displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP inspection</td>
<td>arp-inspection</td>
<td>ARP inspection auto-recovery.</td>
</tr>
<tr>
<td>BPDU Guard</td>
<td>bpduguard</td>
<td>BPDU guard auto-recovery.</td>
</tr>
<tr>
<td>Broadcast Storm</td>
<td>bcast-storm</td>
<td>Broadcast storm auto-recovery.</td>
</tr>
<tr>
<td>BPDU Storm</td>
<td>bpdustorm</td>
<td>BPDU storm auto-recovery.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>denial-of-service</td>
<td>Denial of Service auto-recovery.</td>
</tr>
<tr>
<td>DHCP Rate Limit</td>
<td>dhcp-rate-limit</td>
<td>DHCP rate limit auto-recovery.</td>
</tr>
<tr>
<td>Loop Protection</td>
<td>loop-protect</td>
<td>Loop protection auto-recovery.</td>
</tr>
<tr>
<td>Port MAC Locking</td>
<td>port-security</td>
<td>Port security MAC locking auto-recovery.</td>
</tr>
<tr>
<td>Multicast Storm</td>
<td>mcast-storm</td>
<td>Multicast storm auto-recovery.</td>
</tr>
<tr>
<td>SFP Mismatch</td>
<td>sfp-mismatch</td>
<td>SFP mismatch auto-recovery.</td>
</tr>
<tr>
<td>SFP Plus Mismatch</td>
<td>sfplusr-mismatch</td>
<td>SFP+ transceiver inserted in SFP port auto-recovery.</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>spanning-tree</td>
<td>Spanning-tree auto-recovery.</td>
</tr>
<tr>
<td>UDLD</td>
<td>udlld</td>
<td>UDLD auto-recovery.</td>
</tr>
<tr>
<td>Unicast Storm</td>
<td>ucast-storm</td>
<td>Unicast storm auto-recovery.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>denial-of-service</td>
<td>Denial of Service auto-recovery.</td>
</tr>
</tbody>
</table>
Layer 2 Switching Commands

Command History

Implemented in version 6.3.0.1 firmware. Modified in version 6.5 firmware.

Example

```
console(config)#show errdisable recovery
Reason                  Auto-recovery Status
------------------     ---------------------
ARP Inspection            Disabled
BPDU Guard                Disabled
Broadcast Storm           Disabled
BPDU Storm                Disabled
Denial of Service        Disabled
DHCP Rate Limit          Disabled
Keep Alive               Disabled
Loop Protection          Disabled
Port Security            Disabled
Multicast Storm          Disabled
SFP Mismatch             Disabled
SFP Plus Mismatch        Disabled
Spanning Tree            Disabled
UDLD                     Disabled
Unicast Storm            Disabled
```

Interval for auto-recovery of error disabled interfaces: 300 seconds

```
show interfaces status err-disabled
```

Use the `show interfaces status err-disabled` command to display the interfaces that are error disabled by the system.

Syntax

```
show interfaces status err-disabled
```

Default Configuration

No recovery causes are enabled by default.

<table>
<thead>
<tr>
<th>Term</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval</td>
<td>time interval</td>
<td>Time interval for auto-recovery in seconds.</td>
</tr>
</tbody>
</table>
**Command Mode**

EXEC mode, Privileged Exec mode, and all submodes.

**User Guidelines**

Error disabled interfaces indicate that a problem that must be resolved by the administrator. This could be a configuration problem or a physical problem and does not necessarily indicate a problem with the switch.

When the interval expires, the system examines the error disabled interfaces and recovers them if recovery for the indicated cause is enabled. Only a single timer is used and recovery occurs when the timer expires, not when the interface time expires. The recovery delay time indicates the number of seconds until the interface is eligible for recovery if auto-recovery is enabled for the indicated cause.

Interfaces recovered by auto-recovery issue a log message indicating that recovery is being attempted.

```<13> Sep 25 14:38:32 10.130.135.107-1 UDLD[nim_t]: udld_util.c(1829) 87 %%
Interface Gi1/0/1 is restored from the error disabled state.```

The possible causes for error disabled interfaces are:

<table>
<thead>
<tr>
<th>Term</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP inspection</td>
<td>arp-inspection</td>
<td>ARP inspection auto-recovery.</td>
</tr>
<tr>
<td>BPDU Guard</td>
<td>bpduguard</td>
<td>BPDU guard auto-recovery.</td>
</tr>
<tr>
<td>Broadcast Storm</td>
<td>bcast-storm</td>
<td>Broadcast storm auto-recovery.</td>
</tr>
<tr>
<td>BPDU Storm</td>
<td>bpdustorm</td>
<td>BPDU storm auto-recovery.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>denial-of-service</td>
<td>Denial of Service auto-recovery.</td>
</tr>
<tr>
<td>DHCP Rate Limit</td>
<td>dhcp-rate-limit</td>
<td>DHCP rate limit auto-recovery.</td>
</tr>
<tr>
<td>Loop Protection</td>
<td>loop-protect</td>
<td>Loop protection auto-recovery.</td>
</tr>
<tr>
<td>Port MAC Locking</td>
<td>port-security</td>
<td>Port security MAC locking auto-recovery.</td>
</tr>
<tr>
<td>Multicast Storm</td>
<td>mcast-storm</td>
<td>Multicast storm auto-recovery.</td>
</tr>
</tbody>
</table>
Layer 2 Switching Commands

**Command History**
Implemented in version 6.3.0.1 firmware. Modified in version 6.5 firmware.

**Example**
The following example
```
console#show interfaces status err-disabled
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Reason</th>
<th>Recovery Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>UDLD</td>
<td>279</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>BPDU Guard</td>
<td>285</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>BPDU Storm</td>
<td>291</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP Mismatch</td>
<td>sfp-mismatch</td>
<td>SFP mismatch auto-recovery.</td>
</tr>
<tr>
<td>SFP Plus Mismatch</td>
<td>sfpplus-mismatch</td>
<td>SFP Plus mismatch auto-recovery.</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>spanning-tree</td>
<td>Spanning-tree auto-recovery.</td>
</tr>
<tr>
<td>UDLD</td>
<td>udlld</td>
<td>UDLD auto-recovery.</td>
</tr>
<tr>
<td>Unicast Storm</td>
<td>ucast-storm</td>
<td>Unicast storm auto-recovery.</td>
</tr>
</tbody>
</table>
IPv6 Access List Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Access to a switch or router can be made more secure through the use of Access Control Lists (ACLs) to control the type of traffic allowed into or out of specific ports. An ACL consists of a series of rules, each of which describes the type of traffic to be processed and the actions to take for packets that meet the classification criteria. Rules within an ACL are evaluated sequentially until a match is found, if any. Every ACL is terminated by an implicit deny all rule, which covers any packet not matching a preceding explicit rule. ACLs can help to ensure that only authorized users have access to specific resources while blocking out any unwarranted attempts to reach network resources.

ACLs may be used to restrict contents of routing updates, decide which types of traffic are forwarded or blocked and, above all, provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network.

The Dell EMC Networking ACL feature allows classification of packets based upon Layer 2 through Layer 4 header information. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique EtherType value; thus all IPv6 classifiers implicitly include the EtherType field.

Multiple ACLs per interface are supported. The ACLs can be combination of Layer 2 and/or Layer 3/4 ACLs. ACL assignment is appropriate for both Ethernet ports and LAGs. ACLs can also be time based.

### Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>permit (IPv6 ACL)</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>show ipv6 access-lists</td>
</tr>
<tr>
<td>ipv6 access-list rename</td>
<td>–</td>
</tr>
</tbody>
</table>
deny | permit (IPv6 ACL)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

Syntax

[sequence-number] deny | permit (IPv6 ACL)

[sequence number] {deny | permit} {ipv6-protocol | number | every}
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [{range
{portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-
65535}] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-
address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt |
gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh |
-psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-
type icmp-type [icmp-code icmp-code] | icmp-message icmp-message]
[routing] [fragments] [dscp dscp]}} [time-range time-range-name] [log]
[assign-queue queue-id] [{mirror | redirect} interface-id] [rate-limit rate
burst-size]

no [sequence-number]

- sequence-number — Identifies the order of application of the permit/deny
statement. If no sequence number is assigned, permit/deny statements are
assigned a sequence number beginning at 1000 and incrementing by 10.
Statements are applied in hardware beginning with the lowest sequence
number. Sequence numbers only have applicability within an access group,
i.e. the ordering applies within the access-group scope. The range for
sequence numbers is 1- 2147483647.

- {deny | permit}—Specifies whether the IP ACL rule permits or denies the
matching traffic.

- {ipv6-protocol | number | every}—Specifies the protocol to match for the
IP ACL rule.
  - IPv6 protocols: icmpv6, ipv6, sctp, tcp and udp
  - Every: Match any protocol (don’t care)

- source-ipv6-prefix/prefix-length | any | host src-ipv6-address—Specifies a
source IP address and netmask to match for the IP ACL rule.
  - For IPv6 ACLs, “any” implies a 0:/128 prefix and a mask of all ones.
Specifying “host X::X” implies a prefix length as “/128” and a mask of 0::/128.

- `{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}}`—Specifies the layer 4 destination or source port match condition for the IP/TCP/UDP ACL rule. A source or destination port number, which ranges from 0-65535, can be entered, or a portkey, which can be one of the following keywords: bgp, domain, echo, ftp, ftp-data, http, ntp, pop2, pop3, rip, smtp, snmp, telnet, tftp, telnet, time, who and www. Each of these keywords translates into its equivalent destination port number.

- When “range” is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range.

- When “eq” is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey.

- When “lt” is specified, IPv6 ACL rule matches if the layer 4 destination port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>.

- When “gt” is specified, IPv6 ACL rule matches if the layer 4 destination port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535.

- When “neq” is specified, IPv6 ACL rule matches only if the layer 4 destination port number is not equal to the specified port number or portkey.

- IPv6 TCP port names: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3

- IPv6 UDP port names: domain, echo, ntp, rip, snmp, time, who

- destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address—Specifies a destination IP address and netmask for match condition of the IP ACL rule.
- For IPv6 ACLs, “any” implies 0::/128 prefix and a mask of all ones.
- Specifying host implies prefix length as “/128” and a mask of 0::/128.

• `[dscp dscp]`—Specifies a match of DSCP values.

• `flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]`—Specifies that the IP/TCP/UDP ACL rule matches on the TCP flags.
  - When “+<tcpflagname>” is specified, a match occurs if specified `<tcpflagname>` flag is set in the TCP header.
  - When “-<tcpflagname>” is specified, a match occurs if specified `<tcpflagname>` flag is *NOT* set in the TCP header.
  - When “established” is specified, a match occurs if specified either RST or ACK bits are set in the TCP header.
  - This option is visible only if the protocol is tcp.

  - **Ack** – Acknowledgment bit
  - **Fin** – Finished bit
  - **Psh** – push bit
  - **Rst** – reset bit
  - **Syn** – Synchronize bit
  - **Urg** – Urgent bit

  - When icmp-type is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255.
  - When icmp-code is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255.
  - Specifying icmp-message implies both icmp-type and icmp-code are specified.
  - ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type. This option is visible only if the protocol is “icmpv6”.

– The icmpv6 message types are available only if the protocol is icmpv6.

• flow-label—Specifies a match on the identified flow label. Range 0–1048575.

• fragments—Specifies the rule matches packets that are non-initial fragments (fragment bit asserted). Not valid for rules that match L4 information such as TCP port number since that information is carried in the initial packet. IPv6 fragments contain an IPv6 Fragment extension header.

• routing—Specifies that IP ACL rule matches on routed packets. Routed packets contain an IPv6 “routing” extension header.

• log—Specifies that this rule is to be logged when the rule has been matched one or more times since the expiry of the last logging interval. The logging interval is five minutes.

• time-range time-range-name—Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

• assign-queue queue-id—Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.

• {mirror | redirect} interface-id—Specifies the mirror or redirect Ethernet interface to which packets matching this rule are copied or forwarded, respectively.

• rate-limit rate burst-size—Specifies the allowed rate of traffic as per the configured rate in Kbps, and burst-size in kbytes.

– Rate – the committed rate in kilobits per second
– Burst-size – the committed burst size in Kilobytes.

**Default Configuration**
An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.

**Command Mode**
IPv6-Access-List Configuration mode

**User Guidelines**
A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format. An IPv6 ACL implicitly includes the EtherType in the match criteria. The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The assign-queue parameter is valid only for a permit rule. The command is enhanced to accept the optional time-range parameter. The time-range parameter allows imposing a time limitation on the IPv6 ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist, and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with the specified name exists, and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with a specified name becomes active. The ACL rule is removed when the time-range with a specified name becomes inactive.

Users are permitted to add rules, but if a packet does not match any user-specified rules, the packet is dropped by the implicit “deny all” rule.

In order to provide the greatest amount of flexibility in configuring ACLs, the permit/deny syntax allows combinations of matching criteria that may not make sense when applied in practice.

Any – is equivalent to ::/0 for IPv6 access lists.
Host - indicates /128 prefix length for IPv6.

Port ranges are not supported for egress (out) IPv6 traffic-filters. This means that only the eq operator is supported for egress (out) ACLs.

The protocol type must be SCTP, TCP or UDP to specify a port range. The protocol type must be IPv6, SCTP, TCP, ICMPv6, or UDP to specify a flow label.

The IPv6 “fragment” and “routing” keywords are not supported on egress (out) access groups. The log action is supported for both permit and deny rules.

If a permit|deny clause is entered with the same sequence number as an existing rule, the configuration is denied with an error message.

An implicit deny all condition is added by the system after the last MAC or IP/IPv6 access group if no route-map is configured on the interface.

Every permit/deny rule that does not have a rate-limit parameter is assigned a counter. If counter resources become exhausted, a warning is issued and the rule is applied to the hardware without the counter.

If a permit|deny clause is entered with the same sequence number as an existing rule, an error is displayed and the existing rule is not updated with the new information.

Since ACLs have an implicit deny all at the end of the last access-group, IPv6 ACLs need an explicit permit icmp any any nd-na and permit icmp any any nd-ns statements as match conditions. These additional conditions allow for ICMPv6 neighbor discovery to occur.

For the N4000 series:

- The IPv6 ACL “routing” keyword is not supported when an IPv6 address is specified.
- For ingress (in) ACLs, the IPv6 ACL “fragment” keyword matches only on the first two IPv6 extension headers for the fragment header (next header code 44). If the fragment header appears in the third or subsequent header, it is not matched.

The rate-limit command is not supported for egress (out) access groups.

For the N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON series switches, for ingress (in) ACLs:
• The IPv6 ACL “fragment” keyword matches only on the first IPv6 extension header for the fragment header (next header code 44). If the fragment header appears in the second or a subsequent header, it is not matched.

• The IPv6 ACL “routing” keyword matches only on the first IPv6 extension header for the routing header (next header code 43). If the fragment header appears in the second or a subsequent header, it is not matched.

• For all series switches, port ranges are not supported on egress (out) ACLs. Only the eq operator is supported in an egress ACL.

**Command History**

Updated in 6.3.0.1 firmware.

Example and description updated in the 6.4 release.

**Example**

The following example creates rules in an IPv6 ACL named "STOP_HTTP" to discard any HTTP traffic from the 2001:DB8::0/32 network, but allow all other traffic from that network:

```
console(config)#ipv6 access-list STOP_HTTP
console(Config-ipv6-acl)#deny tcp 2001:DB8::0/32 any eq http
console(Config-ipv6-acl)#permit every
```

**ipv6 access-list**

The `ipv6 access-list` command creates an IPv6 Access Control List (ACL) consisting of classification fields defined for the IP header of an IPv6 frame.

**Syntax**

```
ipv6 access-list name
no ipv6 access-list name
```

• `name` — Alphanumeric string of 1 to 31 characters uniquely identifying the IPv6 access list.

**Default Configuration**

There is no default configuration for this command.
**Command Mode**
Global Configuration mode

**User Guidelines**
The name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL with this name already exists, this command enters Ipv6-Access-List Configuration mode to update the existing IPv6 ACL.

Use the **no** form of the command to delete an IPv6 ACL from the system.

**Example**
The following example creates an IPv6 ACL named “DELL_IP6” and enters the IPv6-Access-List Configuration mode:

```
console(config)#ipv6 access-list DELL_IP6
console(Config-ipv6-acl)#
```

**ipv6 access-list rename**
The **ipv6 access-list rename** command changes the name of an IPv6 Access Control List (ACL). This command fails if an IPv6 ACL with the new name already exists.

**Syntax**
```
ipv6 access-list rename name newname
```

- **name** — the name of an existing IPv6 ACL.
- **newname** — alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Global Configuration mode
**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config)#ipv6 access-list rename DELL_IP6 DELL_IP6_NEW_NAME
```

**ipv6 traffic-filter**

The `ipv6 traffic-filter` command either attaches a specific IPv6 Access Control List (ACL) to an interface or associates it with a VLAN ID in a given direction.

Use the `no` form of the command to remove an IPv6 traffic-filter from the interface(s) in a given direction.

**Syntax**

```
ipv6 traffic-filter name [in | out | control-plane][seq-num]
no ipv6 traffic-filter name [in | out | control-plane]
```

- **name** — An alphanumeric string of 1 to 31 characters uniquely identifying the IPv6 access list.
- **in** — The access list is applied to ingress packets.
- **out** — The access list is applied to egress packets.
- **control-plane** — The access list is applied to ingress control plane packets. This parameter is only available in Global Configuration mode.
- **seq-num** — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1–4294967295)

**Default Configuration**

No IPv6 traffic filters are configured by default.

**Command Modes**

Global Configuration mode, Interface Configuration (Ethernet, Port-channel, VLAN) mode
User Guidelines

Dell EMC Networking switches support configuration of multiple access groups on interfaces. An optional sequence number may be specified to indicate the order of this access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified IPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Configuration mode only affects a single interface, whereas the Global Configuration mode setting is applied to all interfaces. The optional control-plane keyword allows application of an ACL on the CPU port ingress queue. Control plane packets (e.g., BPDUs) are dropped because of the implicit deny all rule added at the end of every access control list. To mitigate this behavior, permit rules must be added by the operator to allow the appropriate control plane packets to ingress the CPU (i.e., ARP, DHCP, LACP, STP BPDU, etc.). The control-plane keyword does not filter traffic received over the out-of-band port.

Example

The following example attaches an IPv6 access control list to an interface.

```
console(config-if-Gi1/0/1)#ipv6 traffic-filter DELL_IP6 in
```

Command History

Syntax updated in the 6.4 release.

show ipv6 access-lists

Use the show ipv6 access-lists command in User Exec and Privileged Exec mode to display an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Syntax

```
show ipv6 access-lists [name]
```
• name—The name used to identify the IPv6 ACL.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```console
console#show ipv6 access-lists

Current number of ACLs: 4  Maximum number of ACLs: 100

<table>
<thead>
<tr>
<th>ACL Name</th>
<th>Rules</th>
<th>Interface(s)</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6-ACL</td>
<td>1</td>
<td>Gi1/0/8</td>
<td>Inbound</td>
</tr>
<tr>
<td>43981900</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>asdasd</td>
<td>2</td>
<td>Gi1/0/7</td>
<td>Inbound</td>
</tr>
<tr>
<td>3981901</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

console#show ipv6 access-lists IPv6-ACL

IPV6 ACL Name: IPv6-ACL

Inbound Interface(s):
Gi1/0/8

Rule Number: 1
Action......................................... permit
Match All...................................... FALSE
Protocol....................................... 6(tcp)
Source IPV6 Address............................ fe80::2121/128
Destination IPV6 Address....................... fe80::2121/128
Destination Layer 4 Operator............... Equal To
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination L4 Port Keyword</td>
<td>800</td>
</tr>
<tr>
<td>Flow Label</td>
<td>65535</td>
</tr>
<tr>
<td>TCP Flags</td>
<td>FIN (Set)</td>
</tr>
<tr>
<td></td>
<td>SYN (Ignore)</td>
</tr>
<tr>
<td></td>
<td>RST (Ignore)</td>
</tr>
<tr>
<td></td>
<td>PSH (Ignore)</td>
</tr>
<tr>
<td></td>
<td>ACK (Ignore)</td>
</tr>
<tr>
<td></td>
<td>URG (Ignore)</td>
</tr>
<tr>
<td>ACL Hit Count</td>
<td>43981900</td>
</tr>
</tbody>
</table>
IPv6 MLD Snooping Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

In IPv6, Multicast Listener Discover (MLD) snooping performs functions similar to IGMP snooping in IPv4. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP. MLD version 1 (MLDv1) is equivalent to IGMPv2. MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

Dell EMC Networking switches can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously. The Dell EMC Networking implementation is compliant to RFC 4541.

Commands in this Section

This section explains the following commands:

- `ipv6 mld snooping vlan groupmembership-interval`
- `ipv6 mld snooping vlan mrouter`
- `ipv6 mld snooping vlan immediate-leave`
- `ipv6 mld snooping (Global)`
- `ipv6 mld snooping listener-message-suppression`
- `show ipv6 mld snooping`
- `ipv6 mld snooping vlan last-listener-query-interval`
- `show ipv6 mld snooping groups`
- `ipv6 mld snooping vlan mctrexpiretime`
- `show ipv6 mld snooping mrouter`
**ipv6 mld snooping vlan groupmembership-interval**

The `ipv6 mld snooping vlan groupmembership-interval` command sets the MLD Group Membership Interval time on a VLAN or interface. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

**Syntax**

```
ipv6 mld snooping vlan vlan-id groupmembership-interval time
no ipv6 mld snooping vlan vlan-id groupmembership-interval time
```

- `vlan-id` — A VLAN identifier (Range 1-4093).
- `time` — MLD group membership interval time in seconds. (Range: 2-3600)

**Default Configuration**

The default group membership interval time is 260 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config)#ipv6 mld snooping vlan 2 groupmembership-interval 1500
```

**ipv6 mld snooping vlan immediate-leave**

This command enables or disables MLD Snooping immediate-leave mode on a selected VLAN.
**Syntax**

ipv6 mld snooping vlan vlan-id immediate-leave

- vlan-id—A VLAN identifier (Range 1-4093).

**Default Configuration**

Immediate leave is disabled on all VLANs by default.

**Command Mode**

Global Configuration mode.

**User Guidelines**

Enabling immediate-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving an MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Enable immediate-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same Layer 2 LAN port, but were still interested in receiving multicast traffic directed to that group. Also, immediate-leave processing is supported only with MLD version 1 hosts.

**Example**

This example enables mld snooping immediate-leave for VLAN 2.

```
console(config)#ipv6 mld snooping vlan 2 immediate-leave
```

**ipv6 mld snooping listener-message-suppression**

This command enables MLD listener message suppression on a specific VLAN. Use the no form of this command to disable listener message suppression.

**Syntax**

ipv6 mld snooping vlan vlan-id listener-message-suppression

no ipv6 mld snooping vlan vlan-id listener-message-suppression

- vlan-id—A VLAN identifier (Range 1-4093).
Default Configuration
Listener message suppression is enabled by default.

Command Mode
Global Configuration mode.

User Guidelines
MLD listener message suppression is equivalent to IGMP report suppression. When MLD listener message suppression is enabled, the switch only sends the first report received for a group in response to a query. Listener message suppression is only applicable to MLDv1.

Example
console(config)#ipv6 mld snooping vlan 10 listener-message-suppression

ipv6 mld snooping vlan last-listener-query-interval

The ipv6 mld snooping vlan last-listener-query-interval command sets the number of seconds after which a host is considered to have left the group.

Syntax
ipv6 mld snooping vlan vlan-id last-listener-query-interval time
no ipv6 mld snooping vlan vlan-id last-listener-query-interval

• vlan-id — A VLAN identifier (Range 1-4093).
• time — The number of seconds after which a host is considered to have left the group. (Range: 1–25 seconds)

Default Configuration
The default maximum response time is 10 seconds.

Command Mode
Global Configuration mode
User Guidelines
This value must be less than the MLD Query Interval time value. The range is 1 to 25 seconds.

Example
console(config)#ipv6 mld snooping vlan 2 last-listener-query-interval 7

ipv6 mld snooping vlan mcrtrexpiretime
The ipv6 mld snooping mcrtrexpiretime command sets the multicast router present expiration time.

Syntax
ipv6 mld snooping vlan vlan-id mcrtrexpiretime time
no ipv6 mld snooping vlan vlan-id mcrtrexpiretime
  • vlan-id — A VLAN identifier (Range 1-4093).
  • time — Multicast router present expiration time in seconds. (Range: 1–3600)

Default Configuration
The default multicast router present expiration time is 300 seconds.

Command Mode
Global Configuration mode.

User Guidelines
The time is set for a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 1 to 3600 seconds.

Example
console(config)#ipv6 mld snooping vlan 2 mcrtrexpiretime 1500
**ipv6 mld snooping vlan mrouter**

This command statically configures a port as connected to a multicast router for a specified VLAN. The no form of this command removes the static binding.

**Syntax**

```
ipv6 mld snooping vlan vlan-id mrouter interface interface
```

```
no ipv6 mld snooping vlan vlan-id mrouter interface interface
```

- **vlan-id** — A VLAN identifier (Range 1-4093).
- **interface-id** — The next-hop interface to the multicast router.

**Default Configuration**

There are no multicast router ports configured by default.

**Command Mode**

Global Configuration mode.

**User Guidelines**

MLD snooping will forward IPv6 multicast data packets in the VLAN if a static mrouter port is configured. This behavior can be used to ensure that MLD snooping will selectively forward IPv6 multicast data traffic even if no dynamically discovered IPv6 multicast router has been discovered.

**Example**

```
console(config)#ipv6 mld snooping vlan 10 mrouter interface Gi1/0/2
```

**ipv6 mld snooping (Global)**

Use the `ipv6 mld snooping (Global)` command to globally enable MLD Snooping on the system (Global Configuration Mode). Use the no form of the command to disable MLD snooping.

**Syntax**

```
ipv6 mld snooping [vlan vlan-id]
```

```
no ipv6 mld snooping [vlan vlan-id]
```
Layer 2 Switching Commands

- vlan-id — A VLAN identifier (Range 1-4093).

Default Configuration
MLD Snooping is enabled globally and on all VLANs by default.

Command Mode
Global Configuration mode.

User Guidelines
Use this command without parameters to globally enable MLD Snooping. Use the no form of the command to disable MLD Snooping. Use the vlan parameter to enable MLD Snooping on a specific VLAN.

It is recommended that IGMP snooping should be enabled whenever MLD snooping is enabled to ensure that unwanted pruning of multicast protocol packets used by other protocols does not occur.

Enabling MLD snooping on an IPv6 L3 multicast router is recommended. If a multicast source is connected to a VLAN on which both L3 multicast and IGMP/MLD snooping are enabled, the multicast source is forwarded to the mrouter ports as well as the internal mrouter port. MLD snooping does not flood IPv6 multicast data plane packets in the VLAN if IPv6 L3 routing is enabled. If MLD snooping is disabled, the switch will flood multicast data plane packets in the VLAN.

Example
console(config)#ipv6 mld snooping
console(config)#no ipv6 mld snooping vlan 1

show ipv6 mld snooping
The show ipv6 mld snooping command displays MLD Snooping information and SSM statistics. Configured information is displayed whether or not MLD Snooping is enabled.

Syntax
show ipv6 mld snooping [interface interface-id | vlan vlan-id]
- interface-id—An Ethernet interface identifier or a port channel identifier
• vlan-id—A VLAN identifier.

**Default Configuration**

This command has no default configuration

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

With no optional arguments, the command displays the following information:

• Admin Mode — Indicates whether or not MLD Snooping is active on the switch.

• Multicast Control Frame Count — Displays the total number of IGMP or PIM packets which have been received (same as IPv4).

• Flooding Unregistered to All Ports — Indicates if Flooding Unregistered to All Ports is enabled. If enabled, multicast data traffic for which no listeners have registered is flooded to all ports in a VLAN instead of only flooded to multicast router ports.

• SSM FDB Capacity — The capacity of the SSM FDB.

• SSM FDB Current Entries — The current count of SSM FDB entries.

• SSM FDB High Water Mark — The highest count of FDB entries since the last clear counters.

When you specify an interface or VLAN, the following information displays:

• MLD Snooping Admin Mode — Indicates whether MLD Snooping is active on the interface or VLAN.

• Fast Leave Mode — Indicates whether MLD Snooping Fast-leave is active on the VLAN.

• Group Membership Interval — Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
• Last Listener Query Interval—Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.

• Multicast Router Present Expiration Time — Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

• Listener Message Suppression Mode—Sends only the first report received in response to a query to the router.

Example

```
console(config)#show ipv6 mld snooping

Admin Mode..................................... Enable
Multicast Control Frame Count.................. 6255
SSM FDB Capacity.................................. 64
SSM FDB High Water Mark......................... 1
SSM FDB Current Entries........................ 1
Flooding Unregistered to All Ports............. Disabled

Vlan 1:
-------
MLD Snooping Admin Mode........................ Enabled
Immediate Leave Mode........................... Disabled
Group Membership Interval...................... 260
Last Listener Query Interval................... 10
Multicast Router Expiry Time.................... 300
Listener Message Suppression Mode............. Enabled
```

**show ipv6 mld snooping groups**

The `show ipv6 mld snooping groups` command displays the MLD Snooping and SSM entries in the MFDB table.

**Syntax**

```
show ipv6 mld snooping groups [{vlan vlan-id | address ipv6-multicast-address}]
```

- vlan-id — A VLAN identifier (Range 1-4093).
- ipv6-multicast-address — Specifies an IPv6 multicast address.
**Default configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This user guideline applies to all switch models. To see the full multicast address table (including static addresses) use the show mac address-table multicast command.

**Example**
This example shows MLDv2 snooping entries

```
console#show ipv6 mld snooping groups

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Type</th>
<th>OIFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3333.0000.0003</td>
<td>Dynamic</td>
<td>Te1/0/1,Te1/0/17</td>
</tr>
</tbody>
</table>

MLD SSM Entries:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Group</th>
<th>Reporter</th>
<th>Filter</th>
<th>IIF</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ff1e:2222:2222:</td>
<td>fe80::200:3ff:f</td>
<td>include</td>
<td>Te1/0/1</td>
<td>2001::2</td>
</tr>
<tr>
<td></td>
<td>2222:2222:2222</td>
<td>e00:b00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

**show ipv6 mld snooping mrouter**
Use the show ipv6 mld snooping mrouter command to display information on dynamically learned multicast router interfaces.

**Syntax**
show ipv6 mld snooping mrouter
Default configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
MLD snooping forwards IPv6 multicast data plane packets to mrouter ports, including statically configured mrouter ports. If a static mrouter port is configured in a VLAN, MLD snooping will forward multicast data plane packets received on the VLAN even if the interface is down. This behavior can be used to ensure that MLD snooping will selectively forward IPv6 multicast data traffic even if no dynamically discovered IPv6 multicast router has been discovered.

Example
console#show ipv6 mld snooping mrouter
VLAN ID  Port
--------  --------
10        Gi1/0/2 (static)
IPv6 MLD Snooping Querier

Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The MLD Snooping Querier is an extension of the MLD snooping feature. MLD Snooping Querier allows the switch to simulate an MLD router in a Layer 2-only network, thus removing the need to have an MLD router to collect the multicast group membership information. The querier function simulates a small subset of the MLD router functionality.

In a network with IP multicast routing, the IP multicast router acts as the MLD querier. However, if it is required that the IP-multicast traffic in a VLAN be switched, the switch can be configured as an MLD querier. When MLD Snooping Querier is enabled, the querier sends out periodic MLD general queries that trigger the multicast listeners/member to send their joins so as to receive the multicast data traffic. MLD snooping listens to these reports to establish the appropriate forwarding table entries.

Commands in this Section

This section explains the following commands:

- `ipv6 mld snooping querier`
- `ipv6 mld snooping querier query-interval`
- `ipv6 mld snooping querier (VLAN mode)`
- `ipv6 mld snooping querier timer expiry`
- `ipv6 mld snooping querier address`
- `show ipv6 mld snooping querier`
- `ipv6 mld snooping querier election participate`
- `-`

**ipv6 mld snooping querier**

Use the `ipv6 mld snooping querier` command to enable MLD Snooping Querier on the system. Use the `no` form of this command to disable MLD Snooping Querier.
Syntax
ipv6 mld snooping querier
no ipv6 mld snooping querier

Default Configuration
MLD Snooping Querier is disabled by default.

Command Mode
Global Configuration mode

User Guidelines
It is not recommended the MLD Snooping Querier be enabled on a switch enabled for IPv6 multicast routing.

Example
console(config)#ipv6 mld snooping querier

ipv6 mld snooping querier (VLAN mode)
Use the ipv6 mld snooping querier command in VLAN mode to enable MLD Snooping Querier on a VLAN. Use the no form of this command to disable MLD Snooping Querier on a VLAN.

Syntax
ipv6 mld snooping querier vlan vlan-id
no ipv6 mld snooping querier vlan vlan-id
  • vlan-id — A VLAN identifier. (Range: 1–4093)

Default Configuration
MLD Snooping Querier is disabled by default on all VLANs.

Command Mode
Global Configuration mode
User Guidelines
There are no user guidelines for this command.

Example
console(config)#ipv6 mld snooping querier vlan 10

ipv6 mld snooping querier address
Use the ipv6 mld snooping querier address command to set the global MLD Snooping Querier address. Use the no form of this command to reset the global MLD Snooping Querier address to the default.

Syntax
ipv6 mld snooping querier address prefix[/prefix-length]
no ipv6 mld snooping querier address
• prefix — An IPv6 address prefix.
• prefix-length — Designates how many of the high-order contiguous bits of the address make up the prefix.

Default Configuration
There is no global MLD Snooping Querier address configured by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)#ipv6 mld snooping querier address Fe80::5
**ipv6 mld snooping querier election participate**

Use the `ipv6 mld snooping querier election participate` command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. Use the `no` form of this command to disable election participation on a VLAN.

**Syntax**

```
ipv6 mld snooping querier election participate vlan-id
no ipv6 mld snooping querier election participate vlan-id
```

- `vlan-id` — A VLAN identifier (Range: 1 - 4093)

**Default Configuration**

Election participation is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

When enabled, if there is another querier in the network and the local querier is in election mode, then the querier with the lower IP address is elected and the other querier stops querying. If the local querier is not in election mode and another querier is detected, the local querier stops querying.

**Example**

```
console(config-vlan)#ipv6 mld snooping querier election participate 10
```

**ipv6 mld snooping querier query-interval**

Use the `ipv6 mld snooping querier query-interval` command to set the MLD Querier Query Interval time. Use the `no` form of this command to reset the Query Interval to the default.

**Syntax**

```
ipv6 mld snooping querier query-interval interval
```

```
ipv6 mld snooping querier query-interval
```

• interval — Amount of time that the switch waits before sending another general query. (Range: 1–1800 seconds)

Default Configuration
The default query interval is 60 seconds.

Command Mode
Global Configuration mode

User Guidelines
The query interval is the amount of time in seconds that the switch waits before sending another general query.

Example
console(config)#ipv6 mld snooping querier 120

ipv6 mld snooping querier timer expiry
Use the ipv6 mld snooping querier timer expiry command to set the MLD Querier timer expiration period. Use the no form of this command to reset the timer expiration period to the default.

Syntax
ipv6 mld snooping querier timer expiry timer
ipv6 mld snooping querier timer expiry

• timer — The time that the switch remains in Non-Querier mode after it has discovered that there is a multicast querier in the network. (Range: 60–300 seconds)

Default Configuration
The default timer expiration period is 60 seconds.

Command Mode
Global Configuration mode
User Guidelines
The timer expiry is the time period that the switch remains in non-querier mode once it has discovered that there is another multicast querier in the network.

Example
console(config)#ipv6 mld snooping querier timer expiry 222

show ipv6 mld snooping querier
Use the show ipv6 mld snooping querier command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Syntax
show ipv6 mld snooping querier [detail | vlan vlan-id]
  • vlan-id — A VLAN identifier (Range: 1 - 4093)

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
When the optional argument vlan vlan-id is not used, the command shows the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD Snooping Querier Mode</td>
<td>Indicates whether or not MLD Snooping Querier is active on the switch.</td>
</tr>
<tr>
<td>Querier Address</td>
<td>Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.</td>
</tr>
</tbody>
</table>
When the optional argument `vlan` `vlan-id` is used, the following additional information appears:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD Snooping Querier VLAN Mode</td>
<td>Indicates whether MLD Snooping Querier is active on the VLAN.</td>
</tr>
<tr>
<td>Querier Election Participate Mode</td>
<td>Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.</td>
</tr>
<tr>
<td>Querier VLAN Address</td>
<td>Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Indicates whether MLD Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in Querier state it will send out periodic general queries. When in Non-Querier state it will wait for moving to Querier state and does not send out any queries.</td>
</tr>
<tr>
<td>Operational Version</td>
<td>Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it can not be changed.</td>
</tr>
<tr>
<td>Operational Max Response Time</td>
<td>Displays the maximum response time the local querier waits for a response from a multicast router.</td>
</tr>
</tbody>
</table>

When the optional argument `detail` is used, the command shows the global information and the information for all Querier enabled VLANs as well as the following information:

| Last Querier Address                  | Indicates the IP address of the most recent Querier from which a Query was received.                |
| MLD Version | Indicates the version of MLD. |
IP Source Guard Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

IP Source Guard (IPSG) is a security feature that filters IP packets based on source ID. The source ID may either be source IP address or a {source IP address, source MAC address} pair. The network administrator configures whether enforcement includes the source MAC address. The network administrator can configure static authorized source IDs. The DHCP Snooping binding database and static IPSG entries identify authorized source IDs. IPSG may be enabled on Ethernet and port-channel ports. IPSG is disabled by default.

If the network administrator enables IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending upon the admin-configured IPSG entries. IPSG cannot be enabled on a port-based routing interface.

IPSG uses two enforcement mechanisms: the L2FDB to enforce the source MAC address and ingress VLAN and an ingress classifier to enforce the source IP address or {source IP, source MAC} pair.

Commands in this Section

This section explains the following commands:

- `ip verify source`  
- `ip verify binding`  
- `show ip verify`  
- `show ip verify source`  
- `show ip source binding`

**ip verify source**

Use the `ip verify source` command in Interface Configuration mode to enable filtering of IP packets from hosts which have not been assigned an IP address via DHCP on the specified interface.

Use the `no` form of the command to enable unverified traffic to flow over the interfaces.
**Syntax**

ip verify source {port-security}

no ip verify source

- **port-security**—Enables filtering based on IP address, VLAN, and MAC address. When not specified, filtering is based upon IP address.

**Default Configuration**

By default, no sources are blocked.

**Command Mode**

Interface Configuration mode (Ethernet and port channel)

**User Guidelines**

DHCP snooping should be enabled on any ports for which **ip verify source** is configured. If **ip verify source** is configured on an interface for which DHCP snooping is disabled, or for which DHCP snooping is enabled and the port is trusted, incoming traffic on the interface is dropped.

Incoming traffic is filtered based on the source IP address and VLAN. When the port-security keyword is configured, filtering occurs based upon source IP address, VLAN and source MAC address.

IP source guard also interacts with the port security component. Use the **switchport port-security** command in interface mode to optionally add checking of learned MAC addresses. When port security is enabled, MAC learning coordinates with the IP Source Guard to verify that the MAC address is in the DHCP binding database. If it is not, port security is notified that the frame is in violation of the security policy.

**Example**

```plaintext
console(config)#ip dhcp snooping
console(config)#ip dhcp snooping vlan 1
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#ip verify source
```
**ip verify binding**

Use the `ip verify binding` command in Global Configuration mode to configure static bindings. Use the no form of the command to remove the IPSG entry.

**Syntax**

```
ip verify binding macaddr vlan ipaddr interface
```

**Default Configuration**

By default, there are no static bindings configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

The configured IP address and MAC address are used to match the source IP address and source MAC address for packets received on the interface. Hosts sending packets using the configured source IP address and source MAC address are trusted on the interface.

**Example**

```
console(config)#ip verify binding 00:11:22:33:44:55 vlan 1 1.2.3.4 interface gigabitethernet 1/0/2
```

**show ip verify**

Use the `show ip verify` command to display the IP Source Guard configuration on all interfaces or the specified interface.

**Syntax**

```
show ip verify [interface interface-id]
```

- interface-id—An Ethernet interface identifier or a port channel interface identifier.
Default Configuration
There is no default configuration for this command.

Command Modes
User Exec, Privileged Exec (all show modes)

User Guidelines
The filter type is one of the following values:

- ipv4-mac: IPv4 plus MAC address filtering
- ip: IPv4 address filtering
- ipv6: IPv6 address filtering
- ipv6-mac: IPv6 plus MAC address filtering
- N/A: No filtering is configured on the interface

Example

```console
console(config-if-Gi1/0/5)#show ip verify

+------------+---------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>ip</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>ipv4-mac</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>ipv4-mac</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>N/A</td>
</tr>
</tbody>
</table>

console(config-if-Gi1/0/5)#show ip verify interface gi1/0/5

+------------+---------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/5</td>
<td>ipv6-mac</td>
</tr>
</tbody>
</table>
```

show ip verify source

Use the `show ip verify source` command to display the bindings configured on a particular interface or all interfaces.
Syntax
show ip verify source [interface interface-id]
  •  interface-id: A valid Ethernet interface identifier or port-channel identifier

Default Configuration
There is no default configuration for this command.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
console#show ip verify source interface gigabitethernet 1/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>ip</td>
<td>1.2.3.4</td>
<td>00:12:32:43:54:66</td>
<td>1</td>
</tr>
</tbody>
</table>

show ip source binding

Use the show ip source binding command to display all bindings (static and dynamic).

Syntax
show ip source binding

Default Configuration
There is no default configuration for this command.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
console#show ip source binding
MAC Address   IP Address Type VLAN Interface
------------- ---------- ----- ----- ---------------
0011.2233.4455 1.2.3.4 static 1   Gi1/0/2
iSCSI Optimization Commands

Dell EMC Networking N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

iSCSI Optimization provides a means of performing configuration specific to storage traffic and optionally giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment.

iSCSI Optimization is best applied to mixed-traffic networks where iSCSI packets constitutes a portion of overall traffic. In these cases, the assignment of iSCSI packets to non-default CoS queues can provide flows with lower latency and avoid queue resource contention.

If iSCSI frames comprise most of the traffic passing through the switch, the system provides optimal throughput when all traffic is assigned to the default queue. An example of this situation is a Storage Area Network (SAN) where the switch is dedicated to interconnecting iSCSI Targets with Initiators. Using the default queue for this homogeneous traffic provides the best performance in traffic burst handling and the most accurate 802.3x Flow Control Pause Frame generation. In these cases, the application of QoS treatment other than the default policy may result in less overall throughput or more packet loss.

By default, iSCSI optimization is enabled and iSCSI QoS treatment is disabled.

LLDP is used to detect the presence of EqualLogic storage arrays. When iSCSI optimization is enabled, and LLDP detects an EQL array on a port, that port configuration is changed to enable portfast and disable unicast storm control. Configuration changes appear in the running config and are not removed by disabling the feature or disconnecting the EQL array.

QoS treatment is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

In addition, if configured, the packets can be updated with IEEE 802.1p or IP-DSCP values. This is done by enabling remark. Remarketing packets with priority data provides special QoS treatment as the packets continue through the network.
iSCSI Optimization borrows ACL lists from the global system pool. ACL lists allocated by iSCSI Optimization reduce the total number of ACLs available for use by the network operator. Enabling iSCSI Optimization uses one ACL list to monitor for iSCSI sessions for the application of any CoS treatment.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iscsi cos</strong></td>
<td>Set the quality of service profile that will be applied to iSCSI flows. To return the VPT/DSCP setting to the default value, use the <code>no</code> form of this command. VPT/DSCP values can be configured independently from the application of QoS treatment.</td>
</tr>
<tr>
<td><strong>show iscsi</strong></td>
<td>–</td>
</tr>
<tr>
<td><strong>iscsi enable</strong></td>
<td>Enable application of preferential QoS treatment to iSCSI frames.</td>
</tr>
</tbody>
</table>

**iscsi cos**

Use the `iscsi cos` command in Global Configuration mode to set the quality of service profile that will be applied to iSCSI flows. To return the VPT/DSCP setting to the default value, use the `no` form of this command. VPT/DSCP values can be configured independently from the application of QoS treatment.

**Syntax**

```
iscsi cos {enable | disable | vpt vpt | dscp dscp} [remark]
```

**no iscsi cos**

- **enable**—Enables application of preferential QoS treatment to iSCSI frames.
- **disable**—Disables application of preferential QoS treatment to iSCSI frames.
- **vpt/dscp**—The VLAN Priority Tag or DSCP value to assign received iSCSI session packets.
- **remark**—Mark the iSCSI frames with the configured DSCP when egressing the switch.

**Default Configuration**

By default, frames are not remarked. The default vpt setting for iSCSI is 4, which the default class of service 802.1p mapping assigns to queue 2.
**Command Mode**

Global Configuration mode.

**User Guidelines**

The remark option only applies to DSCP values. Remarketing is not available for vpt values.

In general, the use of iSCSI CoS is not required. By default, iSCSI flows are assigned to the highest VPT/DSCP value that is mapped to the highest queue not used for stack management or the voice VLAN. Make sure you configure the relevant Class of Service parameters for the queue in order to complete the setting.

Configuring the VPT/DSCP value sets the QoS profile which selects the egress queue to which the frame is mapped. The default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may alter the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. These choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR, the queue to which the flow is assigned to can be set to get the required percentage using the min-bandwidth settings.

If an EqualLogic array is detected when QoS is enabled, two additional TCP ports receive preferential QoS treatment (TCP ports 25555 and 9876). This QoS policy is applied globally. The `iscsi cos enable` command enables the generation of the iSCSI Application Priority TLV over DCBX using the value set by the `iscsi cos vpt` command on switches that support DCBX.

**Example**

The following example configures iSCSI packets to receive CoS treatment using DiffServ Code Point AF 41 and configures remarking of transmitted iSCSI packets.

```
console(config)#iscsi cos dscp 41 remark
```
**iscsi enable**

The `iscsi enable` command globally enables iSCSI optimization. To disable iSCSI optimization, use the `no` form of this command.

**Syntax**

`iscsi enable`

`no iscsi enable`

**Default Configuration**

iSCSI is enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command modifies the running config to enable flow control on all interfaces.

Monitoring for EqualLogic Storage arrays via LLDP is enabled by this command. Upon detection of an EQL array, the specific interface involved will have spanning-tree portfast enabled and unicast storm control disabled. These changes appear in the running config. Disabling iSCSI Optimization does not disable flow control, portfast or storm control configuration applied as a result of enabling iSCSI Optimization.

On the N4000 switches, enabling iSCSI will locally generate a DCBX Application Priority TLV with the following parameters when the following conditions are met:

- DCBX is enabled
- CoS Queuing is enabled on the port using VPT (`iscsi cos enable`)

The Application Priority TLV sent will contain the following information in addition to any other information contained in the TLV:

AE Selector = 1
AE Protocol = 3260
AE Priority = priority configured for iSCSI PFC (the VPT value above). This TLV is sent in addition to any Application Priority TLV information received from the configuration source. If the configuration source is sending iSCSI application priority information, it is not necessary to enable iscsi cos to send the iSCSI Application Priority TLV.

**Command History**
Modified in version 6.5 firmware.

**Example**
In the following example, iSCSI is globally enabled.

```
console(config)#iscsi enable
```

**show iscsi**
Use the `show iscsi` command to display the iSCSI configuration.

**Syntax**
`show iscsi`

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example displays the iSCSI configuration.

```
console#show iscsi
iSCSI enabled
iSCSI CoS disabled
iSCSI vpt is 4
```
Session aging time: 10 min
Maximum number of sessions is 1024

iSCSI Targets and TCP Ports:

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Target IP Address</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

iSCSI Static Rule Table

<table>
<thead>
<tr>
<th>Index</th>
<th>TCP Port</th>
<th>IP Address</th>
<th>IP Address Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9876</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>25555</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
**Link Dependency Commands**

**Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches**

Link dependency allows the link status of a group of interfaces to be made dependent on the link status of other interfaces. The effect is that the link status of a group that depends on another interface either mirrors or inverts the link status of the depended-on interface. Circular dependencies are not allowed. For example, if port-channel 1 in group 1 depends on port-channel 2. Then the system will not allow the operator to configure another link dependency group where port-channel 2 depends on port-channel 1.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Use the action command in Link Dependency mode to indicate if the link-dependency group should mirror or invert the status of the depended-on interfaces.</td>
</tr>
<tr>
<td>link-dependency</td>
<td>depends-on</td>
</tr>
<tr>
<td>add</td>
<td>show link-dependency</td>
</tr>
</tbody>
</table>

**action**

Use the **action** command in Link Dependency mode to indicate if the link-dependency group should mirror or invert the status of the depended-on interfaces.

**Syntax**

```
action {down|up}
```

- **down**—Mirror the depended on interface(s) status.
- **up**—Invert the depended on interface(s) status.

**Default Configuration**

The default configuration for a group is down, i.e. the group members will mirror the depended-on link status by going down when all depended-on interfaces are down.
**Command Mode**
Link Dependency mode

**User Guidelines**
The `action up` command will cause the group members to be up when no depended-on interfaces are up.

**Example**
```
console(config-depend-1)#action up
```

**link-depency-group**
Use the `link-depency-group` command to enter the link-depency mode and configure a link-depency group.

**Syntax**
```
link-depency-group GroupId
no link-depency-group GroupId
```
- `GroupId` — Link dependency group identifier. (Range: 1–72)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
The preference of a group is to remain in the up state. A group will be in the up state if any depends-on interface is up and will be in the down state only if all depends-on interfaces are down.

**Example**
```
console(config)#link-depency-group 1
console(config-linkDep-group-1)#
```
add
Use this command to add member ten Gigabit or Gigabit Ethernet port(s) or port channels to the dependency list.

Syntax
add intf-list

• intf-list — List of Ethernet interface identifiers or port channel identifiers or ranges. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports.

Default Configuration
This command has no default configuration.

Command Mode
Link Dependency mode

User Guidelines
Adding an interface to a dependency list brings the interface down until the depends-on command is entered. The link status will then follow the interface specified in the depends-on command.
To avoid bringing down interfaces, enter the depends-on command prior to entering the add command.

Example
console(config-depend-1)#add gigabitethernet 1/0/1
console(config-depend-1)#add tengigabitethernet 1/0/1
console(config-depend-1)#add port-channel 10-12

depends-on
Use this command to add the dependent Ethernet ports or port channels list. Use the no depends-on command to remove the dependent Ethernet ports or port-channels list.

Syntax
depends-on intf-list
no depends-on intf-list
  • intf-list — List of Ethernet interface identifiers or port channel interface identifiers or ranges. Separate nonconsecutive items with a comma and no spaces. Use a hyphen to designate the range of ports or port-channel numbers.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Link Dependency mode

**User Guidelines**
Circular dependencies are not allowed, i.e. interfaces added to the group may not also appear in the depends-on list of the same group or a different group. If an interface appears in the add list of any group, the interfaces in the corresponding depends-on list may not refer back to the interfaces in the add group.

**Examples**
```
console(config-linkDep-group-1)#depends-on gigabitethernet 1/0/10
console(config-linkDep-group-1)#depends-on port-channel 6
```

**show link-dependency**
Use the `show link-dependency` command to show the link dependencies configured for a particular group. If no group is specified, then all the configured link-dependency groups are displayed.

**Syntax**
```
show link-dependency [group GroupId] [detail]
  • GroupId—Link dependency group identifier. (Range: Valid Group Id, 1–16)
  • detail—Show detailed information about the state of members and the dependent ports.
```
**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

Configure a link dependency group prior to using this command.

**Example**

The following command shows link dependencies for all groups.

```
console#show link-dependency
GroupId Member Ports Ports Depended On Link Action Group State
-------- -----------------------------------------------------
1       Gi4/0/2-3,Gi4/0/5 Gi4/0/10-12 Link Up Up/Down
```

The following command shows link dependencies for group 1 only.

```
console#show link-dependency group 1
GroupId Member Ports Ports Depended On Link Action Group State
-------- -----------------------------------------------------
1       Gi4/0/2-3,Gi4/0/5 Gi4/0/10-12 Link Up Up/Down
```

The following command shows detailed information for group 1.

```
console#show link-dependency group 1 detail
GroupId: 1
Link Action: Link Up
State: Up
Ports Depended On State:
Link Up: Gi4/0/10
Link Down: Gi4/0/11-12
Member Ports State:
Link Up: Gi4/0/2-3
Link Down: Gi4/0/5
```
LLDP Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The IEEE 802.1AB standard defines the Link Layer Discovery Protocol (LLDP). This protocol allows stations residing on an IEEE802 LAN to advertise major capabilities, physical descriptions, and management information to physically adjacent devices, allowing a network management system (NMS) to access and display this information.

The standard is designed to be extensible, providing for the optional exchange of organizational specific information and data related to other IEEE standards. The base implementation supports only the required basic management set of type length values (TLVs).

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function. The information is received and processed by stations implementing the receive function. Devices are not required to implement both transmit and receive functions and each function can be enabled or disabled separately by the network manager. Dell EMC Networking supports both the transmit and receive functions in order to support device discovery.

The LLDP component transmit and receive functions can be enabled/disabled separately per physical port. By default, both transmit and receive functions are enabled on all ports. The application starts each transmit and receive state machine appropriately based on the configured status and operational state of the port.

The transmit function is configurable with respect to packet construction and timing parameters. The required Chassis ID, Port ID, and Time to Live (TTL) TLVs are always included in the Link Layer Discovery Protocol Data Unit (LLDPDU). However, inclusion of the optional TLVs in the management set is configurable by the administrator. By default, they are not included. The transmit function extracts the local system information and builds the LLDPDU based on the specified configuration for the port. In addition, the administrator has control over timing parameters affecting the TTL of LLDPDUs and the interval in which they are transmitted.
The receive function accepts incoming LLDPDU frames and stores information about the remote stations. Both local and remote data may be displayed by the user interface and retrieved using SNMP as defined in the LLDP MIB definitions. The component maintains one remote entry per physical network connection.

The LLDP component manages a number of statistical parameters representing the operation of each transmit and receive function on a per-port basis. These statistics may be displayed by the user interface and retrieved using SNMP as defined in the MIB definitions.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear lldp remote-data</th>
<th>lldp notification-interval</th>
<th>show lldp local-device</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lldp statistics</td>
<td>lldp receive</td>
<td>show lldp med</td>
</tr>
<tr>
<td>deb enable</td>
<td>lldp timers</td>
<td>show lldp med interface</td>
</tr>
<tr>
<td>debug lldp</td>
<td>lldp transmit</td>
<td>show lldp med local-device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td>lldp med</td>
<td></td>
<td>show lldp med remote-device</td>
</tr>
<tr>
<td>lldp med confignotification</td>
<td>lldp tlv-select</td>
<td>show lldp remote-device</td>
</tr>
<tr>
<td>lldp med faststartrepeatcount</td>
<td>show lldp</td>
<td>show lldp statistics</td>
</tr>
<tr>
<td>lldp med transmit-tlv</td>
<td>show lldp interface</td>
<td>–</td>
</tr>
<tr>
<td>lldp notification</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

**clear lldp remote-data**

Use the `clear lldp remote-data` command to delete all LLDP peer information.

**Syntax**

clear lldp remote-data
Default Configuration
By default, data is removed only on system reset.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
The following example displays how to clear the LLDP remote data.

```
console#clear lldp remote-data
```

clear lldp statistics
Use the `clear lldp statistics` command to reset all LLDP statistics.

Syntax
`clear lldp statistics`

Default Configuration
By default, the statistics are only cleared on a system reset.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
The following example displays how to reset all LLDP statistics.

```
console#clear lldp statistics
```
**dcb enable**

This command enables the sending of DCBX information in LLDP frames.

**Syntax**

dcb enable

no dcb enable

**Command Mode**

Global Configuration mode

**Default Value**

The sending of DCBX information is enabled by default.

**User Guidelines**

Use this command to disable the sending of DCBX information when it is desirable to utilize legacy QoS and disable the automatic configuration of CNAs based on transmitted DCBX information.

This command is equivalent to issuing `lldp tlv-select dbx` command on all Ethernet interfaces.

**Example**

console(config)#no dcb enable

**debug lldp**

Use the `debug lldp` command to display LLDP debug information. Use the `no` form of the command to halt the display of LLDP debug information.

**Syntax**

debug lldp packet [transmit | receive]

no debug lldp packet [transmit | receive]

- Transmit–Display LLDP packets transmitted by the switch.
- Receive–Display LLDP packets received by the switch.
Default Configuration
If neither transmit nor receive is specified, packets for both directions are displayed.

Command Mode
Privileged Exec mode

User Guidelines
Decode of LLDP packet information is limited. If possible, it is preferable to attach the Wireshark tool to the switch CPU to obtain a full decode, if an out-of-band port is available. Refer to the Remote Capture example in the User’s Configuration Guide.

Command History
Command introduced in version 6.5 firmware.

lldp med
This command is used to enable/disable LLDP-MED on an interface. By enabling MED, the transmit and receive functions of LLDP are effectively enabled.

Syntax
lldp med
no lldp med

Command Mode
Interface Configuration (Ethernet) mode

Default Value
Transmission and reception of LLDP-MED TLVs is enabled on all supported interfaces.

User Guidelines
No specific guidelines.
**Example**

```console
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)#lldp med
```

**lldp med confignotication**

This command is used to enable sending topology change notifications.

**Syntax**

```lldp med confignotication```

```no lldp med confignotication```

**Command Mode**

Interface Configuration (Ethernet) mode

**Default Value**

By default, notifications are disabled on all Ethernet interfaces.

**User Guidelines**

There are no guidelines for this command.

**Example**

```console
console(config)#lldp med confignotication
```

**lldp med faststartrepeatcount**

This command is used to set the value of the fast start repeat count.

**Syntax**

```lldp med faststartrepeatcount count```

```no lldp med faststartrepeatcount```

- **count** — Number of LLDPPDUs that are transmitted when the protocol is enabled. (Range 1–10)

**Command Mode**

Global Configuration
**Default Value**

3

**User Guidelines**

No specific guidelines.

**Example**

```
console(config)# lldp med faststartrepeatcount 2
```

**lldp med transmit-tlv**

This command is used to specify which optional TLVs in the LLDP MED set are transmitted in the LLDPDUs. There are certain conditions that have to be met for a port to be MED compliant. These conditions are explained in the normative section of the ANSI/TIA-1057 specification. For example, the MED TLV 'capabilities' is mandatory. By disabling transmission of the MED capabilities TLV, MED is effectively disabled on the interface.

**Syntax**

```
lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd]
no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd]
```

**Command Mode**

Interface Configuration (Ethernet)

**User Guidelines**

The optional ex-pse (extended PSE) and ex-pd (extended PD) parameters are only available on PoE capable switches.

**Default Value**

By default, the capabilities and network policy TLVs are included in LLDP packets sent on interfaces enabled for MED. On PoE capable switches, the extended PD TLV and extended PSE TLV are transmitted.

**Example**

```
console(config)#interface gigabitethernet 1/0/1
```
Console(config-if-Gi1/0/1)#lldp med transmit-tlv capabilities
Console(config-if-Gi1/0/1)#lldp med transmit-tlv network-policies

**lldp notification**

Use the **lldp notification** command in Interface Configuration mode to enable remote data change notifications. To disable notifications, use the **no** form of this command.

**Syntax**

```
lldp notification
no lldp notification
```

**Default Configuration**

By default, notifications are disabled on all supported interfaces.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays how to enable remote data change notifications.

```
console(config-if-Gi1/0/3)#lldp notification
```

**lldp notification-interval**

Use the **lldp notification-interval** command in Global Configuration mode to limit how frequently remote data change notifications are sent. To return the notification interval to the factory default, use the **no** form of this command.

**Syntax**

```
lldp notification-interval interval
```

no lldp notification-interval

- interval — The smallest interval in seconds at which to send remote data change notifications. (Range: 5–3600 seconds)

**Default Configuration**
The default value is 5 seconds.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays how to set the interval value to 10 seconds.

```
console(config)#lldp notification-interval 10
```

**lldp receive**
Use the `lldp receive` command in Interface Configuration mode to enable the LLDP receive capability. To disable reception of LLDPDUs, use the `no` form of this command.

**Syntax**

```
lldp receive
no llldp receive
```

**Default Configuration**
The default lldp receive mode is enabled.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**
This command has no user guidelines.
Example
The following example displays how to enable the LLDP receive capability.

```
console(config-if-Gi1/0/3)#lldp receive
```

**lldp timers**

Use the `lldp timers` command in Global Configuration mode to set the timing parameters for local data transmission on ports enabled for LLDP. To return any or all parameters to factory default, use the `no` form of this command.

**Syntax**

```
lldp timers [interval transmit-interval] [hold hold-multiplier] [reinit reinit-delay]
no lldp timers [interval] [hold] [reinit]
```

- transmit-interval — The interval in seconds at which to transmit local data LLDPDUs. (Range: 5–32768 seconds)
- hold-multiplier — Multiplier on the transmit interval used to set the TTL in local data LLDPDUs. (Range: 2–10)
- reinit-delay — The delay in seconds before reinitialization. (Range: 1–10 seconds)

**Default Configuration**

The default transmit interval is 30 seconds.
The default hold-multiplier is 4.
The default delay before reinitialization is 2 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.
**Examples**

The following example displays how to configure LLDP to transmit local information every 1000 seconds.

```
console(config)#lldp timers interval 1000
```

The following example displays how to set the timing parameter at 1000 seconds with a hold multiplier of 8 and a 5 second delay before reinitialization.

```
console(config)#lldp timers interval 1000 hold 8 reinit 5
```

**lldp transmit**

Use the `lldp transmit` command in Interface Configuration mode to enable the LLDP advertise (transmit) capability. To disable local data transmission, use the `no` form of this command.

**Syntax**

`lldp transmit`

`no lldp transmit`

**Default Configuration**

LLDP is enabled on all supported interfaces.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays how enable the transmission of local data.

```
console(config-if-Gi1/0/3)#lldp transmit
```
lldp tlv-select

Use the `lldp tlv-select` command to specify which optional type-length-value settings (TLVs) in the 802.3 AB basic management set will be transmitted in the LLDPDUs. To disable transmission of an optional TLV, use the `no` form of this command. To return the configuration to the default, use the `no` form of the command with no arguments.

**Syntax**

```
lldp tlv-select [dcbxp] [management-address] [port-description] [port-vlan] [system-capabilities] [system-description] [system-name]
```

```
no lldp tlv-select [dcbxp] [management-address] [port-description] [port-vlan] [system-capabilities] [system-description] [system-name]
```

- **dcbxp** — Transmits the Data Center Exchange Protocol TLVs.
- **management-address** — Transmits the switch management address (TLV type 8).
- **port-description** — Transmits the port description (TLV type 4).
- **port-vlan** — Transmits the port PVID (TLV type 127, subtype 1)
- **system-name** — Transmits the system name (TLV type 5).
- **system-description** — Transmits the system description (TLV type 6).
- **system-capabilities** — Transmits the system capabilities (TLV type 7).

**Default Configuration**

By default, the chassis ID (1), port ID (2), time-to-live (3), port-description (4), port-vlan (127/1), and system-name (5) TLVs are transmitted.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

LLDP must be enabled globally, or if disabled globally, enabled on the interface for this command to have an effect.

The switch does not attempt to identify if the transmitted VLAN information matches the received VLAN information.
The string configured by the `hostname` command is transmitted by the system-name TLV.

If no TLV argument is given, the configuration remains unchanged.

Use the `show lldp remote-device all` command to see the advertised LLDP neighbor information.

The management address TLV is type 8. The switch will send the address of the service port, if available, otherwise, the IP address of the switch, if defined, otherwise, the MAC address of the switch. The interface numbering subtype sent is always IfIndex. If IPv6 management addresses are configured, they are also sent.

See the `lldp med` command for additional LLDP transmission capabilities.

**Data Center Bridging**

The capability is only available on the N4000 Series switches.

The DCBX TLVs transmitted are as follows:

- Ets-config—Transmit the ETS configuration TLV.
- Ets-recommend—Transmit the ETS recommendation TLV.
- Pfc—Transmit the PFC configuration TLV.
- Application-priority—Transmit the application priority TLV.
- Congestion-notification—Transmit the congestion notification TLV.

The command `lldp tlv-select dcbxp interface configuration` command configures a port in the same manner as the global configuration `dcb enable` command.

**Command History**

Syntax updated in version 6.5. Deprecated `lldp transmit-tlv` command in favor of `lldp tlv-select` command in 6.5.2 firmware release. Deprecated `lldp transmit-mgmt` command in favor of `lldp tlv-select management-address` in 6.5.2 firmware release.

**Example**

The following example shows how to include the system description TLV in local data transmit.

```
console(config-if-Gi1/0/3)#lldp transmit-tlv system-description
```
**show lldp**

Use the `show lldp` command to display the current LLDP configuration summary.

**Syntax**

`show lldp`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the current LLDP configuration summary.

```console
console#show lldp
LLDP Global Configuration
Transmit Interval............................ 30 seconds
Transmit Hold Multiplier..................... 4
Reinit Delay..................................... 2 seconds
Notification Interval........................ 5 seconds
```

**Command History**

Example updated in the 6.4 release.

**show lldp interface**

Use the `show lldp interface` command to display the current LLDP interface state.
**Syntax**

```
show lldp interface {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port | all}
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

This example show how the information is displayed when you use the command with the `all` parameter.

```
console#show lldp interface all

LLDP Interface Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>Transmit</th>
<th>Receive</th>
<th>Notify</th>
<th>TLVs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>Up</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>Up</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/13</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/15</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/16</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
<tr>
<td>Gi1/0/17</td>
<td>Down</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1,4</td>
</tr>
</tbody>
</table>
```
show lldp interface Gi1/0/1
Interface Link Transmit Receive Notify TLVs Mgmt
--------- ---- -------- -------- -------- ------- ----
Gi1/0/1   Up   Enabled  Enabled  Enabled  0,1,2,4  Y
TLV Codes: 0 – Port Description, 1 – System Name, 2 – System Description, 3 – System Capabilities, 4 – Port VLAN

**show lldp local-device**

Use the `show lldp local-device` command to display the advertised LLDP local data. This command can display summary information or detail for each interface.

**Syntax**

`show lldp local-device {detail interface | interface | all}

- **detail** — includes a detailed version of the local data.
- **interface** — Specifies a valid Ethernet interface on the device. Specify either `gigabitethernet` unit/slot/port or `tengigabitethernet` unit/slot/port or `fortygigabitethernet` unit/slot/port.
- **all** — Shows lldp local device information on all interfaces.

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Examples
These examples show advertised LLDP local data in two levels of detail.

```
console#show lldp local-device all
LLDP Local Device Summary
Interface    Port ID              Port Description
--------- -------------------- --------------------
Gi1/0/1     Gi1/0/1

console# show lldp local-device detail Gi1/0/1
LLDP Local Device Detail
Interface: Gi1/0/1
Chassis ID Subtype: MAC Address
Chassis ID: 00:62:48:00:00:00
Port ID Subtype: Interface Name
Port ID: Gi1/0/1
Port VLAN: 22
System Name:
System Description: Routing
Port Description:
System Capabilities Supported: bridge, router
System Capabilities Enabled: bridge
Management Address:
Type: IPv4
Address: 192.168.17.25
```

show lldp med
This command displays a summary of the current LLDP MED configuration.

Syntax
show lldp med
**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**Default Value**
Not applicable

**User Guidelines**
No specific guidelines.

**Example**
console(config)#show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

**show lldp med interface**
This command displays a summary of the current LLDP MED configuration for a specific interface.

**Syntax**
show lldp med interface {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | all}
- all — Shows information for all valid LLDP interfaces.

**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**Default Value**
Not applicable

**Example**
console#show lldp med interface all
LLDP MED Interface Configuration
Interface Link configMED operMED ConfigNotify TLVsTx
--------- ------ ---------- ---------- ---------------

LLDP MED Interface Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>configMED</th>
<th>operMED</th>
<th>ConfigNotify</th>
<th>TLVsTx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Up</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
</tbody>
</table>

TLV Codes: 0- Capabilities, 1- Network Policy, 2- Location, 3- Extended PSE, 4- Extended PD, 5- Inventory

**show lldp med local-device detail**

This command displays the advertised LLDP local data in detail.

**Syntax**

show lldp med local-device detail {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port}

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**Default Value**

Not applicable

**Example**

Console#show lldp med local-device detail gi1/0/8

LLDP MED Local Device Detail

Interface: Gi1/0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
Layer 2 Switching Commands

show lldp med remote-device

This command displays the current LLDP MED remote data. This command can display summary information or detail for each interface.
Syntax

show lldp med remote-device {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | all}
show lldp med remote-device detail {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port}

• all — Indicates all valid LLDP interfaces.
• detail — Includes a detailed version of remote data for the indicated interface.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

Default Value

Not applicable

Example

console#show lldp med remote-device all

LLDP Remote Device Summary
Local
Interface  RemoteID  Device Class
---------  ---------  -------------------
Gi1/0/13   1         Class I
Gi1/0/16   2         Class II
Gi1/0/23   6         Not Defined

Console#show lldp med remote-device detail Gi1/0/1
LLDP MED Remote Device Detail

Local Interface: 1/0/1

Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low

**show lldp remote-device**

Use the `lldp remote-device` command to display the current LLDP remote data. This command can display summary information or detail for each interface.
**Syntax**

`show lldp remote-device {detail interface | interface | all}`

- `detail` — Includes detailed version of remote data.
- `interface` — Specifies a valid Ethernet interface on the device. Substitute `gigabithernet unit/slot/port` or `tengabithernet unit/slot/port` or `fortygabithernet unit/slot/port`.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

These examples show current LLDP remote data, including a detailed version.

```console
console#show lldp remote-device all

LLDP Remote Device Summary

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>RemID</th>
<th>Chassis ID</th>
<th>Port ID</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/19</td>
<td>7</td>
<td>00:1E:C9:AA:AB:FD</td>
<td>Gi1/0/5</td>
<td></td>
</tr>
</tbody>
</table>
```

```console
console#show lldp remote-device detail Gi1/0/19

LLDP Remote Device Detail

Local Interface: Gi1/0/19
```
show lldp statistics

Use the show lldp statistics command to display the current LLDP traffic statistics.

**Syntax**

show lldp statistics {unit/slot/port | all}

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

The following examples shows an example of the display of current LLDP traffic statistics. The output is abbreviated for the all form of the command.

console#show lldp statistics all

LLDP Device Statistics

Last Update................................. 0 days 22:58:29
Total Inserts.................................. 1
Total Deletes.................................. 0
Total Drops.................................. 0
Total Ageouts................................ 1

<table>
<thead>
<tr>
<th>Tx</th>
<th>Rx</th>
<th>Interface</th>
<th>Total Discards</th>
<th>Errors</th>
<th>Ageout</th>
<th>TLV</th>
<th>TLV</th>
<th>TLV</th>
<th>TLV</th>
<th>TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Gi1/0/1</td>
<td>29395</td>
<td>82562</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

console#show lldp statistics Gi1/0/7

LLDP Device Statistics

Last Update.................................. 0 days 00:38:16
Total Inserts.................................. 13
Total Deletes.................................. 0
Total Drops.................................. 0
Total Ageouts................................ 0

<table>
<thead>
<tr>
<th>Tx</th>
<th>Rx</th>
<th>Interface</th>
<th>Total Discards</th>
<th>Errors</th>
<th>Ageout</th>
<th>TLV</th>
<th>TLV</th>
<th>TLV</th>
<th>TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Gi1/0/7</td>
<td>2297</td>
<td>2298</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The following table explains the fields in this example.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update</td>
<td>The value of system of time the last time a remote data entry was created, modified, or deleted.</td>
</tr>
<tr>
<td>Total Inserts</td>
<td>The number of times a complete set of information advertised by a remote device has been inserted into the table.</td>
</tr>
<tr>
<td>Total Deletes</td>
<td>The number of times a complete set of information advertised by a remote device has been deleted from the table.</td>
</tr>
<tr>
<td>Fields</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Drops</td>
<td>Number of times a complete set of information advertised by a remote device could not be inserted due to insufficient resources.</td>
</tr>
<tr>
<td>Total Ageouts</td>
<td>Number of times any remote data entry has been deleted due to time-to-live (TTL) expiration.</td>
</tr>
<tr>
<td>Transmit Total</td>
<td>Total number of LLDP frames transmitted on the indicated port.</td>
</tr>
<tr>
<td>Receive Total</td>
<td>Total number of valid LLDP frames received on the indicated port.</td>
</tr>
<tr>
<td>Discards</td>
<td>Number of LLDP frames received on the indicated port and discarded for any reason.</td>
</tr>
<tr>
<td>Errors</td>
<td>Number of non-valid LLDP frames received on the indicated port.</td>
</tr>
<tr>
<td>Ageouts</td>
<td>Number of times a remote data entry on the indicated port has been deleted due to TTL expiration.</td>
</tr>
<tr>
<td>TLV Discards</td>
<td>Number LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.</td>
</tr>
<tr>
<td>TLV Unknowns</td>
<td>Number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.</td>
</tr>
<tr>
<td>TLV MED</td>
<td>Number of OUI specific MED (Media Endpoint Device) TLVs received.</td>
</tr>
<tr>
<td>TLV</td>
<td>Number of OUI specific TLVs received.</td>
</tr>
<tr>
<td>TLV 802.3</td>
<td>Number of OUI specific 802.3 specific TLVs received.</td>
</tr>
<tr>
<td>TLV UPOE</td>
<td>Number of PoE TLVs received.</td>
</tr>
</tbody>
</table>
Loop Protection

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Loop protection detects physical and logical loops between Ethernet ports on a device. Loop protection must be enabled globally before it can be enabled at the interface level.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive (Interface Config)</td>
<td>show keepalive</td>
</tr>
<tr>
<td>keepalive (Global Config)</td>
<td>show keepalive statistics</td>
</tr>
<tr>
<td>keepalive action</td>
<td>–</td>
</tr>
</tbody>
</table>

**keepalive (Interface Config)**

Use the `keepalive` command in Interface Configuration mode to enable loop protection on an interface. Use the `no` form of the command to return the configuration to the defaults.

**Syntax**

`keepalive`

`no keepalive`

**Default Configuration**

Loop protection is disabled globally by default and disabled on all interfaces by default.

**Command Mode**

Interface (Ethernet) Configuration mode
**User Guidelines**

Loop protection operates by unicasting a Configuration Test Protocol (CTP) reply packet with the following field settings:

- Source MAC Address: Switch L3 MAC address
- Destination MAC Address: Switch L3 MAC address
- Ether Type: 0x0900 (LOOP)
- Skip Count: 0
- Functions: Reply
- Receipt Number: 0
- Data: 0

Since all switch ports share the same MAC address, if any interface receives CTP packets transmitted by the switch in excess of the configured limit, that interface is error disabled with a Loop Protection cause.

Looped CTP packets received on a routed interface are ignored and will not error-disable the interface. This is because routed interfaces receiving a packet addressed to the router will not unicast flood the packet to the VLAN.

The switch never sends a response to received CTP packets. The switch may flood the first few CTP packets it receives until a MAC address entry is placed in the CAM.

The CTP protocol operates on physical Ethernet interfaces only. It does not operate over Link Aggregation Groups. It may be configured to operate on LAG members.

The CTP protocol does not operate over the out-of-band interface.

**Command History**

Implemented in version 6.3.0.1 firmware.

**Example**

The following example enables loop protection on an interface:

```plaintext
console(config)#keepalive
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#keepalive
```

This example disables loop protection on an interface:
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#no keepalive

**keepalive (Global Config)**

Use the `keepalive` command in Global Configuration mode to enable keepalive or to configure the loop protection timer and packet count. Use the `no` form of the command to return the configuration to the defaults.

**Syntax**

```
keepalive [ period [ count ] ]
no keepalive
```

- **period** – Configures the interval for the transmission of keepalive packets.
  Default: 10 seconds
- **count** – Configures the number of consecutive CTP packets addressed to and received by the local switch before the interface is error disabled.
  Default: 3 packets.

**Default Configuration**

Loop protection is disabled globally by default.
The default period is 10 seconds.
The default count is 3 packets.

**Command Mode**

Global Configuration mode

**User Guidelines**

Loop protect must be enabled individually on a physical interface as well as globally.
If only the period parameter is specified, the count parameter remains unchanged.
Loop protection may only be enabled on physical interfaces, not on port channels or any virtual interfaces.
Command History
Implemented in version 6.3.0.1 firmware.

Example
The following example configures the CTP transmit interval to transmit CTP packets every 5 seconds.

```
console(config)#keepalive 5
```

This example configures the CTP transmit interval to 5 seconds. If an interface receives two CTP packets, it error disables the interface.

```
console(config)#keepalive 5 2
```

In the next example, if the CTP transmit interval is configured to 5 seconds, if an interface receives three CTP packets, it will error disable the interface.

```
console(config)#no keepalive
```

keepalive action
Use the `keepalive action` command to configure the action taken when a loop is detected on an interface. Use the `no` form of the command to return the action to the default.

Syntax

```
keepalive action {error-disable | log-only}
no keepalive action
```

- `error-disable` — When a loop is detected, the interface is disabled and a log message is issued.
- `log-only` — When a loop is detected, a log message is issued and the interface is not error disabled.

Default Configuration
The default is to error disable the interface when a loop is detected.
Command Mode
Interface Configuration mode

User Guidelines
Error disabled interfaces can be configured to auto-recover using the errdisable recovery cause loop-protect command. Keepalive should only be configured on interfaces that do not participate in spanning-tree. Keepalive may disable interfaces in the spanning-tree designated (blocked) role.

Command History
Implemented in version 6.3.0.1 firmware. Syntax corrected in 6.4 release.

Example
The following example configures loop protection to log detected loop conditions without error disabling the port.

```
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#keepalive action log-only
```

show keepalive
Use the show keepalive command to display the global loop protect configuration.

Syntax
show keepalive

Default Configuration
There is no default configuration.

Command Mode
Privileged Exec mode and configuration submodes.

User Guidelines
The following information is displayed.
Layer 2 Switching Commands

Command History
Implemented in version 6.3.0.1 firmware. Example updated in 6.4 version.

Example
console#show keepalive

Keepalive Service.............................. Enabled
Transmit Interval.............................. 10
Retry Count.................................... 3

show keepalive statistics

Use the show keepalive statistics command to display the loop protect status for one or all interfaces.

Syntax
show keepalive statistics {interface-id | all}

- interface-id — Displays the statistics for the specified Ethernet (Physical) interface.
- all — Displays statistics for all interfaces.

Default Configuration
There is no default configuration.

Command Mode
Privileged Exec mode and all configuration sub modes
**User Guidelines**

The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface identifier.</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>Are keepalives transmitted on this interface (Yes, No)?</td>
</tr>
<tr>
<td>Loop Detected</td>
<td>Has a loop been detected (Yes, No)?</td>
</tr>
<tr>
<td>Loop Count</td>
<td>The number of CTP packets detected.</td>
</tr>
<tr>
<td>Time Since Last Loop</td>
<td>The last time a loop was detected.</td>
</tr>
<tr>
<td>Rx Action</td>
<td>Action when a loop is detected (Error disable, Log).</td>
</tr>
<tr>
<td>Port Status</td>
<td>Current port status (Enable, Disable).</td>
</tr>
</tbody>
</table>

**Command History**

Implemented in version 6.3.0.1 firmware.

**Example**

```
console#show keepalive statistics gi1/0/3
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Keep Alive</th>
<th>Loop Detected</th>
<th>Loop Count</th>
<th>Time Since Last Loop</th>
<th>Rx Action</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/0/3</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td>Error disable</td>
<td>Enable</td>
</tr>
</tbody>
</table>
MLAG Commands

Dell EMC Networking N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

MLAG enables a LAG to be created across two independent switches, so that some member ports of a MLAG can reside on one switch and the other members of a MLAG can reside on another switch. The partner switch on the remote side can be a MLAG-unaware unit. To the MLAG unaware switch, the MLAG appears to be a single LAG connected to a single switch.

Commands in this Section

This section explains the following commands:

| clear vpc statistics                      | show vpc consistency-parameters          |
| feature vpc                               | show vpc consistency-features            |
| peer detection enable                     | show vpc peer-keepalive                  |
| peer detection interval                   | show vpc role                            |
| peer-keepalive destination                | show vpc statistics                      |
| peer-keepalive enable                     | system-mac                               |
| peer-keepalive timeout                    | system-priority                          |
| role priority                             | vpc                                      |
| show vpc                                  | vpc domain                               |
| show vpc brief                            | vpc peer-link                            |

clear vpc statistics

Use the clear vpc statistics command to clear the counters for the keepalive messages transmitted and received by the MLAG switch.

Syntax

clear vpc statistics {peer-keepalive | peer-link}
Default Configuration
There is no default configuration for this command.

Command Modes
Privileged Exec mode

User Guidelines
There are no user guidelines for this command.

Example
console#clear vpc statistics

feature vpc
The feature vpc command globally enables MLAG. Use the no form of the command to globally disable MLAG.

Syntax
feature vpc
no feature vpc

Default Configuration
By default, the MLAG feature is not globally enabled.

Command Modes
Global Configuration mode

User Guidelines
The MLAG configuration is retained even when the feature is disabled. The peer link will not be enabled if the VPC feature is not enabled.
MLAG role election occurs if the MLAG feature is enabled and the keepalive state machine is enabled.

Example
console#configure terminal
console(config)#feature vpc
peer detection enable

Use the **peer detection enable** command to enable the Dual Control Plane Detection Protocol. This enables the detection of peer MLAG switches and suppresses state transitions out of the secondary state in the presence of peer link failures.

Use the **no** form of the command to disable the dual control plane detection protocol.

**Syntax**

peer detection enable
no peer detection enable

**Default Configuration**

Dual Control Plane Detection Protocol is disabled by default.

**Command Modes**

MLAG Domain Configuration mode

**Usage Guidelines**

Use of the Dual Control Plane Detection Protocol is optional. It provides a second layer of redundancy beyond that provided by the peer link protocol. System that operate without the DCPDP protocol enabled (and use static LAGs) run the risk of a split brain scenario in the case of peer link failure.

**Example**

```
console(config)#vpc domain 1
console(config-vpc 1)#peer-keepalive enable
console(config-vpc 1)#peer-keepalive destination 192.168.0.2 source 192.168.0.1
console(config-vpc 1)#peer detection enable
console(config-vpc 1)#exit
```

peer detection interval

Use this command to configure the peer detection transmission interval and the detection interval. Use the **no** form of the command to return the transmission and detection intervals to the default.
Syntax

peer detection interval interval-msecs timeout timeout-msecs

no peer detection interval

• interval-msecs—The peer keepalive timeout in seconds. The range is 200–4000 milliseconds.
• timeout-msecs—The peer timeout value in milliseconds. The range is 700–14000 milliseconds.

Default Configuration

The default transmission interval is 1000 milliseconds. The default reception timeout is 3500 milliseconds.

Command Modes

VPC Domain mode

User Guidelines

This command configures the DCPDP transmission and timeout values. If an MLAG switch does not receive DCPDP messages from the peer for the configured timeout value, it takes the decision to transition its role (if required).

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-vpc 1)#peer detection interval 750 timeout 3000

peer-keepalive destination

Use the peer-keepalive destination command to enable the Dual Control Plane Detection Protocol with the configured IP address of the peer MLAG, the local source address and the peer timeout value. The UDP port on which the MLAG switch listens to the Dual Control Plane Detection Protocol messages is also configurable with this command.

Use the no form of the command to return the configuration to the default.
Syntax
peer-keepalive destination ipaddress source srcaddr [udp-port port]
no peer-keepalive destination

- ipaddress—The IP address of the MLAG peer.
- port—The UDP port number to use to listen for peer Dual Control Plane Detection Protocol packets.
- srcaddr—The local source address to use.

Default Configuration
There are no Dual Control Plane Detection Protocol peers configured by default.

Command Modes
MLAG Domain Configuration mode

User Guidelines
Changes to the DCPDP configuration do not take effect until the protocol is disabled and then re-enabled. Both the local switch and the MLAG peer switch must be configured identically. The recommended procedure to update these parameters is to disable the DCPDP protocol on both switches, configure the new parameters on both switches, and then re-enable the DCPDP protocol on both switches.

The Dual Control Plane Detection Protocol is a UDP-based protocol. The administrator must configure this protocol on an IP interface with a VLAN that is not shared with any of the MLAG interfaces. This can include the out-of-band port. When enabled, the dual-control plane detection protocol sends a control plane detection message to the peer once every second. The message is unidirectional and contains the sender’s MAC address. When a switch receives a control plane detection message it sets the ‘peer is UP’ variable to TRUE to indicate that a peer is detected.

Do not configure DCPDP to use a port reserved by the switch. UDP, TCP and RAW ports reserved by the switch and unavailable for use or configuration are:

Ports 1, 17, 58, 255, 546, 547, 2222, 4567, 6343, 49160
Example
console(config)#vpc domain 1
console(config-vpc 1)#peer-keepalive enable
console(config-vpc 1)#peer-keepalive destination 192.168.0.2 source 192.168.0.1
console(config-vpc 1)#peer detection enable
console(config-vpc 1)#exit

peer-keepalive enable

Use the peer-keepalive enable command to enable the peer keepalive protocol on the peer link. When enabled, if an MLAG switch does not receive keepalive messages from the peer within the timeout value and DCPDP is disabled, the switch begins the process of transitioning to the primary role (if standby).

Use the no form of the command to disable the peer keepalive protocol.

Syntax

peer-keepalive enable
no peer-keepalive enable

Default Configuration

The peer keepalive protocol is disabled by default.

Command Modes

MLAG Domain Configuration mode

User Guidelines

MLAG will not become operational until the peer keepalive protocol detects a peer and syncs the peer information. Peer keepalive timeout state transitions are suppressed if the Dual Control Plan Detection (DCPDP) is enabled and detects that the peer is still alive.

Two failure situations cause state transitions:

- The peer device fails: A peer does not receive any more advertisements and the timeout timer expires.
• Secondary device fails: All MLAG members’ port information regarding the secondary device that the primary switch maintains are removed from the primary switch. Forwarding and control processing continues on the local MLAG ports on the primary switch. Once the secondary comes back up again, it starts the keepalive protocol and, if successful in contacting the primary device, moves to the secondary state. It then initiates an FDB sync and becomes operational again.

• Primary device fails: The secondary device transitions to primary state and continues forwarding traffic on its local MLAG ports. It also starts processing control messages. The MLAG connected devices see a change in the source MAC address. Once the peer device comes up again, it starts the keepalive protocol and transitions to the secondary state.

• The peer-link fails: This occurs when either switch cannot contact the peer through the peer keepalive protocol and the DCPDP protocol. The secondary switch transitions to a primary role which results in two primary switches. Both primaries continue forwarding traffic. Each primary also processes control traffic and sends LACP and BPDU packets with a unique source MAC address (the system MAC of the local switch). The MLAG connected devices become aware that they are connected to two devices and, if LACP is enabled, block the links to one of the peers as a new actor ID is received. STP re-convergence may also occur in this scenario.

Example

```
console(config)#vpc domain 1
console(config-vpc 1)#peer-keepalive enable
console(config-vpc 1)#peer-keepalive destination 192.168.0.2 source 192.168.0.1
console(config-vpc 1)#peer detection enable
console(config-vpc 1)#exit
```

**peer-keepalive timeout**

Use this command to configure the peer keepalive timeout value, in seconds. Use the *no* form of this command to return the timeout value to the default.

**Syntax**

```
peer-keepalive timeout value
```
no peer-keepalive timeout
  • value—The peer keepalive timeout value in seconds. The range is 2 to 15 seconds.

Default Configuration
By default, the keepalive timeout value is 5 seconds.

Command Modes
VPC Domain

User Guidelines
This command configures the peer keepalive timeout value (in seconds). If an MLAG switch does not receive keepalive messages from the peer for this timeout value, it takes the decision to transition its role (if required). The keepalive state machine is not restarted if keepalive priority is modified post election.

Command History
Introduced in version 6.2.0.1 firmware.

Example
  console(config-vpc 1)# peer-keepalive timeout 10

role priority
Use the role priority command to configure the priority value used on a switch for primary/secondary role selection. The primary switch is responsible for maintaining and propagating spanning-tree and link-aggregation to the secondary switch.
Use the no form of the command to return the switch priority to the default value.

Syntax
role priority value
no role priority
• Value—The local switch priority value. (The range is 1-255.)

**Default Configuration**

The default priority value is 100.

**Command Modes**

MLAG Domain Configuration mode

**User Guidelines**

This value is used for the MLAG role election and is sent to the MLAG peer in the MLAG keepalive messages. The MLAG switch with the numerically lower priority value becomes the Primary and the switch with higher priority becomes the Secondary. If both the MLAG peer switches have the same role priority, the device with lower system MAC address becomes the Primary switch.

Changes to the priority value are not preemptive. The keepalive role selection state machine is not restarted even if the keepalive priority is modified post election. This means that priority value changes in a running MLAG domain do not affect the selection of the primary and secondary switches. In order for changes to take effect, disable the VPC with the `no feature vpc` command and re-enable it.

**Example**

```
console(config-vpc 1)#role priority 30
```

**show vpc**

Use the `show vpc` command to display MLAG information. The configuration and operational modes of the MLAG are displayed. The MLAG is operationally enabled if all preconditions are met. The port channel configured as an MLAG interface is also displayed along with the member ports on the current switch and peer switch (plus their link status).

**Syntax**

```
show vpc id
```

• id—A valid MLAG identifier.
**Default Configuration**
There is no default configuration for this command.

**Command Modes**
Privileged Exec mode and above

**User Guidelines**
There are no user guidelines for this command.

**Example**

```plaintext
(console)# show vpc 10
VPC Id 10
-----------------
Configuration mode......................Enabled
Operational mode........................Enabled
Port channel...............................Po1

Self member ports        Status
------------------------  ---------
Gi1/0/2                  Up
Gi1/0/6                  Down
```

**show vpc brief**

Use the `show vpc brief` command to display the MLAG global status. The command displays the current MLAG operational mode as well as the peerlink and keepalive status is also displayed. The number of configured and operational MLAGs along with the system MAC and role are also displayed.

**Syntax**

```
show vpc brief
```

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Privileged Exec mode and above
**User Guidelines**

A VPC domain ID must be configured for this command to display the VPC status.

Only the Primary switch maintains the member status of the Secondary switch. The Secondary switch does not maintain or show the status of the Primary switch peer members.

A VPC instance may show as enabled even if all of the port-channels that are members of the VPC are disabled or all of the links in the port channels are disabled. A VPC will show as disabled if peer-link (or DCPDP) connectivity is lost.

The Keepalive admin status field shows the status of the peer-link protocol.

The VPC operational status shows the overall MLAG status.

The Peer detection admin status field shows the status of the DCPDP protocol.

**Example**

```
console#show vpc brief

VPC domain id is not configured.

console#show vpc brief
VPC Domain ID...................................2
VPC admin status................................Disabled
Keepalive admin status..........................Disabled
VPC operational status..........................Disabled
Self role.........................................None
Peer role.........................................None
Peer detection admin status......................Disabled
Operational VPC MAC.........................F8B1.562B.A1D6
Operational VPC system priority............100

Peer-Link details
-----------------

Interface.....................................Po1
Peer-link admin status.......................Enabled
Peer-link STP admin status....................Disabled
Configured VLANs...............................1,10,11,12,13,14,15,16,17
```

VPC Details
-----------
Number of VPCs configured...................... 2
Number of VPCs operational.................... 2

VPC id# 1
----------
Interface...................................... Po2
Configured Vlans............................... 1,10,11,12,13,14,15,16,17
VPC Interface State............................ Active
Local MemberPorts Status
-------------------- -------
Gi1/0/23 UP
Gi1/0/24 UP
Peer MemberPorts Status
-------------------- -------
Gi1/0/23 UP
Gi1/0/24 UP

VPC id# 2
----------
Interface...................................... Po3
Configured Vlans............................... 1,10,11,12,13,14,15,16,17
VPC Interface State............................ Active

show vpc consistency-parameters

Use the show vpc consistency parameters on both MLAG peers to display
MLAG related configuration information in a format suitable for comparison
with the other MLAG peer.

Syntax

show vpc consistency-parameters { global | interface port-channel-number }
  • port-channel-number—A valid port-channel identifier.

Default Configuration

There is no default configuration for this command.

Command Modes

Privileged Exec mode and above
User Guidelines

There are no user guidelines for this command.

Command History

Introduced in 6.2.0.1 firmware.
Updated in 6.3.0.1 firmware.

Example

```
console# show vpc consistency-parameters global

Parameter                    Value
---------------------        -------------------------------------------
STP Mode                     Enabled
STP Version                  IEEE 802.1s
BPDU Filter Mode             Enabled
BPDU Guard Mode              Enabled
MST Instances                1,2,4
FDB Aging Time               300 seconds
VPC System MAC Address       <AA:BB:CC:DD:EE:FF>
VPC System Priority          32767
VPC System MAC Address       00:1E:C9:DE.A2:08
VPC System Priority          32767
VPC Domain ID                1
MST VLAN Configuration

Instance       Associated VLANs
-------------  -----------------------------------
1              7,8,10,20
2              4,5,40-50
4              30,32,34-38

RSTP-PV Configuration

Direct Rapid Convergence:  Enabled/Disabled
DRC Update Rate:  <0-32000> per second
Indirect Rapid Convergence:  Enabled/Disabled

VLAN    STP       STP    Hello     Forward   Maximum   Priority
       Mode   Root    Time     Time      Age        --------
-----  --------   -------   -----     -------   --------  -----------
4      Enabled   Primary   2      15       15        0

switch# show vpc consistency-parameters interface port-channel 2
```
Parameter Name | Value
--- | ---
Port Channel Mode | Enabled
STP Mode | Enabled
BPDU Filter Mode | Enabled
BPDU Flood Mode | Enabled
Auto-edge | FALSE
TCN Guard | True
Port Cost | 2
Edge Port | True
Root Guard | True
Loop Guard | True
Hash Mode | 3
Minimum Links | 1
Channel Type | Static
Configured VLANs | 4,5,7,8
MTU | 1518

Active Port | Speed | Duplex
--- | --- | ---
Gi1/0/1 | 100 | Full
Gi1/0/2 | 100 | Full

MST VLAN Configuration

Instance | Associated VLANS
--- | -------------------
1 | 7,8
2 | 4,5

RSTP-PV Configuration:

STP Port Priority: | <0-240>

VLAN | Port Priority | Cost
--- | --- | ---
<ID> | | <0-240>

show vpc consistency-features

Use the show vpc consistency parameters on both MLAG peers to display MLAG related configuration information in a format suitable for comparison with the other MLAG peer.
Syntax
show vpc consistency-features { global | interface port-channel-number }
  • port-channel-number—A valid port-channel identifier.

Default Configuration
There is no default configuration for this command.

Command Modes
Privileged Exec mode and above

User Guidelines
There are no user guidelines for this command.

show vpc peer-keepalive
Use the show vpc peer-keepalive command to display the peer MLAG switch’s IP address used by the Dual Control Plane Detection Protocol. The port used for the Dual Control Plane Detection Protocol is shown, as well as if peer detection is enabled or not. If enabled, the detection status is displayed.

Syntax
show vpc peer-keepalive

Default Configuration
There is no default configuration for this command.

Command Modes
Privileged Exec mode and above

User Guidelines
A VPC domain ID must be configured for this command to display the keepalive status.

Example
(Switching) # show vpc peer-keepalive
show vpc role

Use the show vpc role command to display information about the keepalive status and parameters. The role of the MLAG switch as well as the system MAC and priority are displayed.

**Syntax**

show vpc role

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Privileged Exec mode and above

**User Guidelines**

A VPC domain ID must be configured for this command to display the VPC role.

**Example**

```console
console# show vpc role
Self
----
VPC domain ID.................................1
Keepalive config mode........................Enabled
Keepalive operational mode....................Enabled
Role Priority................................100
Configured VPC MAC..........................<AA:BB:CC:DD:EE:FF>
Operational VPC MAC..........................<AA:BB:CC:DD:EE:FF>
```
Configured VPC system priority................. 32767
Operational VPC system priority.................. 32767
Local System MAC...................................... 00:10:18:82:18:63
Timeout................................................ 5
VPC State................................................ Primary
VPC Role................................................ Primary

show vpc statistics

Use the `show vpc statistics` command to display the counters for the keepalive messages transmitted and received by the MLAG switch.

Syntax

`show vpc statistics {peer-keepalive | peer-link}`

Default Configuration

There is no default configuration for this command.

Command Modes

Privileged Exec mode and above

User Guidelines

There are no user guidelines for this command.

Example

```
(console)# show vpc statistics peer-keepalive
Total transmitted.................................... 123
Tx successful.......................................... 118
Tx errors................................................ 5
```
Layer 2 Switching Commands

Total received..........................................115
Rx successful...........................................108
Rx Errors.................................................7
Timeout counter........................................6

(console)# show vpc statistics peer-link
Peer link control messages transmitted...............123
Peer link control messages Tx errors..................5
Peer link control messages Tx timeout................4
Peer link control messages ACK transmitted..........34
Peer link control messages ACK Tx errors............5
Peer link control messages received.................115
Peer link data messages transmitted...............123
Peer link data messages Tx errors..................5
Peer link data messages Tx timeout................4
Peer link data messages ACK transmitted..........34
Peer link data messages ACK Tx errors............5
Peer link BPDU’s transmitted to peer...............123
Peer link BPDU’s Tx error.........................9
Peer link BPDU’s received from peer...............143
Peer link BPDU’s Rx error.........................1
Peer link LACPDU’s transmitted to peer...........123
Peer link LACPDU’s Tx error....................9
Peer link LACPDU’s received from peer...........143
Peer link LACPDU’s Rx error....................1

(console)# show vpc statistics peer-link
Peer link control messages transmitted.............24
Peer link control messages Tx errors................0
Peer link control messages Tx timeout...............0
Peer link control messages ACK transmitted..........23
Peer link control messages ACK Tx errors...........0
Peer link control messages received.............23
Peer link data messages transmitted........73
Peer link data messages Tx errors...................0
Peer link data messages Tx timeout...............0
Peer link data messages received............73
Peer link BPDU's transmitted to peer.............0
Peer link BPDU's Tx errors...........................0
Peer link BPDU's received from peer...............0
Peer link BPDU's Rx errors...........................0
Peer link LACPDU's transmitted to peer...........73
Peer link LACPDU's Tx errors....................0
Peer link LACPDU's received from peer...........73
Peer link LACPDU's Rx errors....................0
**system-mac**

Use this command to manually configures the MAC address for the VPC domain. Use the no form of the command to revert the domain MAC address to the default value.

**Syntax**

system-mac mac-address  
no system-mac  

-  mac-address—The system MAC address for the VPC domain.

**Default Configuration**

By default, the domain uses a pre-configured MAC address.

**Command Modes**

VPC domain mode

**User Guidelines**

The VPC domain MAC address must be the same on both MLAG peer devices. The MAC address is a unicast MAC address in aa:bb:cc:dd:ee:ff format and is not equal to the physical MAC address of either the primary VPC or secondary VPC device. The configured VPC domain MAC address is exchanged during role election and, if configured differently on the peer devices, VPC does not become operational.

The configured domain MAC address is present in the LACP PDUs and STP BPDUs that are sent on VPC member ports if VPC primary device election takes place after the VPC MAC address is configured. When the VPC MAC address is configured after the VPC primary device is elected, already agreed upon operational VPC MAC address is used in the LACP PDUs and STP BPDUs instead of the configured VPC MAC address.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-vpc 1)system-mac 00A2.64B3.A245
```
system-priority

Use this command to manually configure the priority for the VPC domain. Use the no form of the command to revert the priority to the default value.

Syntax

system-priority priority
no system-priority

- priority—the priority for the VPC domain. Range is 1-65535.

Default Configuration

By default, the system priority is 32767.

Command Modes

VPC domain mode

User Guidelines

The system priority must be configured identically on all VPC peers. If the configured VPC system priority is different on any VPC peer, the VPC will not come up.

The system-priority is present in the LACP PDUs that are sent out on VPC member ports. When the VPC system priority is configured after a VPC primary device is elected, the already agreed operational VPC system priority is used in the LACP PDUs instead of the newly configured VPC system priority.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-vpc 1) system-priority 2774
vpc

Use the `vpc` command to configure a port-channel (LAG) as part of an MLAG instance. Upon issuing this command, the port-channel is down until the port-channel member information is exchanged and agreed between the MLAG peer switches.

Use the `no` form of the command to remove the LAG from the MLAG domain.

**Syntax**

```
vpc vpc-id
no vpc vpc-id
```

- `vpc-id`—The MLAG identifier.

**Default Configuration**

LAGs are not members of an MLAG domain by default. It is expected that all links belonging to an MLAG instance are connected to switch (or switches) which consider the links to be members of a single LAG.

This configuration must be present on both the primary and secondary switches.

The port channel number and VPC number can be different from each other but the mapping must be the same on the primary and secondary MLAG peers (i.e., the port channel number must map to the same VPC number on both MLAG peers).

**Command Modes**

Port-channel mode

**User Guidelines**

The peer keepalive protocol is required for MLAG operation. Configure a LAG between the two MLAG peers as an MLAG peer link before executing this command.

**Example**

```
console(config)#interface po3
console(config-if-Po3)#switchport mode trunk
```
vpc domain

Use the vpc domain command to enter into MLAG configuration mode. This command creates an MLAG domain and enters into MLAG configuration mode. Use the no form of the command to delete the VPC domain, disable peer-keepalive and peer detection in the domain, and reset all the configured parameters (role priority, VPC MAC address and VPC system priority) for the VPC domain.

Syntax

vpc domain domain-id

• domain-id—The MLAG domain instance. The range is 1-255.

Default Configuration

By default, no MLAG domains are configured.

Command Modes

Global Configuration mode

User Guidelines

Only one MLAG domain per MLAG is supported. This command creates a VPC domain with the specified domain-id and enters into the VPC domain configuration mode. Only one VPC domain can be created on a given device. The domain-id of the VPC domain should be equal to the one configured on the other VPC peer with this device wants to form a VPC pair. The configured VPC domain-ids are exchanged during role election and if they are configured differently on the peer devices, then VPC does not become operational.

The administrator needs to ensure that the no two VPC domains share the same VPC domain-id. The domain-id is used to derive the auto-generated VPC MAC address used in the actor ID field in the LACP PDUs and STP
BPDUs sent out on VPC interfaces. If two VPC domains have the identical domain-ids, the resulting actor IDs may lead to LACP or STP convergence issues.

**Example**

```
console(config)#vpc domain 1
console(config-vpc 1)#peer-keepalive enable
console(config-vpc 1)#peer-keepalive destination 192.168.0.2 source 192.168.0.1
console(config-vpc 1)#peer detection enable
console(config-vpc 1)#exit
```

**vpc peer-link**

Use the `vpc peer-link` command to configure a port channel as the MLAG peer link for a domain and enables the peer link protocol.

Use the **no** form of the command to remove the peer link configuration from an MLAG domain and disable the peer link protocol.

**Syntax**

```
vpc peer-link
no vpc peer-link
```

**Default Configuration**

There are no peer links configured by default.

**Command Modes**

Port-channel configuration mode

**User Guidelines**

This configuration must the present on both the primary and secondary switches. The peer keepalive protocol is required for MLAG operation. Configure and enable a LAG between the two MLAG peers as an MLAG peer link before executing this command.

**Example**

```
console(config)#interface port-channel 1
console(config-if-Po1)#description "MLAG-Peer-Link"
```
console(config-if-Po1)#spanning-tree disable
console(config-if-Po1)#switchport mode trunk
console(config-if-Po1)#switchport trunk allowed vlan 1-99,101-4093
console(config-if-Po1)#vpc peer-link
console(config-if-Po1)#exit
Multicast VLAN Registration Commands

Dell EMC Networking N1100-ON/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Multicast VLAN registration (MVR) is a method for consolidating multicast traffic from multiple VLANs onto a single VLAN. A typical usage scenario would be the distribution of a multicast group to a switch using a single VLAN where the switch has users in different VLANs subscribing to the multicast group. MVR enables the distribution of the multicast group from the single consolidated VLAN onto the multiple user VLANs.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently from each other. Both protocols may be enabled on the switch interfaces at the same time. In such a case, MVR is listening to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- Source port is the port to which the multicast traffic is flowing using the multicast VLAN.
- Receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch will perform VLAN tag substitution from the multicast VLAN Source port to the VLAN tag used by the receiver port.

The multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It must be manually specified by the operator for all multicast source ports in the network. It is this VLAN that is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs.

NOTE: MVR can only be enabled on physical interfaces, not on LAGs or VLANs.

Commands in this Section

This section explains the following commands:
Layer 2 Switching Commands

---

**mvr**

Use the `mvr` command in Global Configuration and Interface Configuration modes to enable MVR. Use the `no` form of this command to disable MVR.

**Syntax**

```
  mvr
  no mvr
```

**Default Configuration**

The default value is `Disabled`.

**Command Mode**

Global Configuration, Interface Configuration

**User Guidelines**

MVR can only be configured on physical interfaces.

**mvr group**

Use the `mvr group` command in Global Configuration mode to add an MVR membership group. Use the `no` form of the command to remove an MVR membership group.

**Syntax**

```
  mvr group A.B.C.D [count]
```

---

**mvr type**

**mvr vlan group**

**show mvr**

**show mvr members**

**show mvr interface**

**show mvr traffic**
no mvr group A.B.C.D [count]

- A.B.C.D—Specify a multicast group.
- count—Specifies the number of multicast groups to configure. Groups are configured contiguously by incrementing the first group specified.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration

**User Guidelines**

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>None</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>• Not an IP multicast group address</td>
</tr>
<tr>
<td></td>
<td>• Illegal IP multicast group address</td>
</tr>
</tbody>
</table>

**Example**

console(config)#mvr
console(config)#mvr group 239.0.1.0 31
console(config)#mvr vlan 10

**mvr mode**

Use the `mvr mode` command in Global Configuration mode to change the MVR mode type. Use the `no` form of the command to set the mode type to the default value.

**Syntax**

mvr mode {compatible | dynamic}

no mvr mode

- compatible—Do not allow membership joins on source ports.
• **dynamic**—Send IGMP joins to the multicast source when IGMP joins are received on receiver ports.

**Default Configuration**
The default mode is compatible.

**Command Mode**
Global Configuration

**User Guidelines**
This command has no user guidelines.

**mvr querytime**
Use the `mvr querytime` command in Global Configuration mode to set the MVR query response time. The query time is the maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group after receiving a leave message. The query time only applies to receiver ports and is specified in tenths of a second.

Use the `no` form of the command to set the MVR query response time to the default value.

**Syntax**

- `mvr querytime 1–100`
- `no mvr querytime`

**Default Configuration**
The default value is 5 tenths of a second.

**Command Mode**
Global Configuration

**User Guidelines**
The following table lists the completion messages.
**mvr vlan**

Use the `mvr vlan` command in Global Configuration mode to set the MVR multicast VLAN. Use the `no` form of the command to set the MVR multicast VLAN to the default value.

**Syntax**

`mvr vlan` `vlan-id`

`no mvr vlan`

- `vlan-id`—Specifies the port on which multicast data is expected to be received. Source ports should belong to this VLAN.

**Default Configuration**

The default value is 1.

**Command Mode**

Global Configuration

**User Guidelines**

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>Defaulting MVR query response time.</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>None</td>
</tr>
</tbody>
</table>

**Example**

```
console(config)#interface Gi1/0/1
console(config-if-Gi1/0/1)#switchport access vlan 2
console(config-if-Gi1/0/1)#mvr
console(config-if-Gi1/0/1)#mvr type receiver
console(config-if-Gi1/0/1)#exit
console(config)#mvr mode dynamic
console(config)#mvr querytime 10
```
mvr immediate

Use the mvr immediate command in Interface Configuration mode to enable MVR Immediate Leave mode. Use the no form of this command to set the MVR multicast VLAN to the default value.

Syntax
mvr immediate
no mvr immediate

Default Configuration
The default value is Disabled.

Command Mode
Interface Configuration

User Guidelines
Immediate leave should only be configured on ports with a single receiver. When immediate leave is enabled, a receiver port will leave a group on receipt of a leave message. Without immediate leave, upon receipt of a leave message, the port sends an IGMP query and waits for an IGMP membership report.

Example
console(config)#interface Gi1/0/1
console(config-if-Gi1/0/1)#switchport access vlan 10
console(config-if-Gi1/0/1)#mvr
console(config-if-Gi1/0/1)#mvr type receiver
console(config-if-Gi1/0/1)#mvr immediate
console(config-if-Gi1/0/1)#exit
console(config)#mvr mode dynamic

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>MVR multicast VLAN ID is set to the default value which is equal to 1.</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>Receiver port in mVLAN, operation failed.</td>
</tr>
</tbody>
</table>
**mvr type**

Use the **mvr type** command in Interface Configuration mode to set the MVR port type. Use the **no** form of this command to set the MVR port type to **None**.

**Syntax**

```plaintext
mvr type {receiver | source}
```

```plaintext
no mvr type
```

- **receiver**—Configure the port as a receiver port. Receiver ports are ports over which multicast data will be sent but not received.
- **source**—Configure the port as a source port. Source ports are ports over which multicast data is received or sent.

**Default Configuration**

The default value is **None**.

**Command Mode**

Interface Configuration

**User Guidelines**

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>None</td>
</tr>
</tbody>
</table>
| Error Completion Message      | • Port is a Trunk port, operation failed.  
                               | • Receiver port in mVLAN, operation failed.             |

**Example**

```plaintext
console(config)#mvr
casele(config)#mvr group 239.1.1.1
casele(config)#vlan 99
casele(config-vlan99)#exit
casele(config)#interface Gi1/0/1
casele(config-if-Gi1/0/1)#switchport access vlan 10
casele(config-if-Gi1/0/1)#mvr
```
mvr vlan group

Use the **mvr vlan group** command in Interface Configuration mode to participate in the specific MVR group. Use the **no** form of this command to remove the port participation from the specific MVR group.

**Syntax**

```
mvr vlan vlan-id group A.B.C.D
no mvr vlan vlan-id group A.B.C.D
```

- **vlan-id**—The VLAN over which multicast data from the specified group is to be received.
- **A.B.C.D.**—The multicast group for which multicast data is to be received over the specified VLAN.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration

**User Guidelines**

This command statically configures a port to receive the specified multicast group on the specified VLAN. This command only applies to receiver ports in compatible mode. It also applies to source ports in dynamic mode. In dynamic mode, receiver ports can also join multicast groups using IGMP messages.

**Example**

```
console(config)#vlan 2000
```
console(config-vlan2000)#exit
console(config)#mvr vlan 2000
console(config)#interface gi1/0/24
console(config-if-Gi1/0/24)#switchport mode trunk
console(config-if-Gi1/0/24)#switchport trunk native vlan 2000
console(config-if-Gi1/0/24)#switchport trunk allowed vlan add 2000
console(config-if-Gi1/0/24)#mvr
console(config-if-Gi1/0/24)#mvr type source
console(config-if-Gi1/0/24)#mvr vlan 2000 group 239.1.1.1

**show mvr**

Use the `show mvr` command to display global MVR settings.

**Syntax**

`show mvr`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>None</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>MVR disabled</td>
</tr>
</tbody>
</table>

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Running</td>
<td>MVR running state. It can be enabled or disabled.</td>
</tr>
<tr>
<td>MVR Multicast VLAN</td>
<td>Current MVR multicast VLAN. It can be in the range from 1 to 4093.</td>
</tr>
</tbody>
</table>
Example

console #show mvr
MVR Running......................... TRUE
MVR multicast VLAN................... 1200
MVR Max Multicast Groups.............. 64
MVR Current multicast groups.......... 1
MVR Global query response time........ 10 (tenths of sec)
MVR Mode................................ compatible

show mvr members

Use the **show mvr members** command to display the MVR membership groups allocated.

Syntax

show mvr members [A.B.C.D]

- A.B.C.D—A valid multicast address in IPv4 dotted notation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Max Multicast Groups</td>
<td>The maximum number of multicast groups that is supported by MVR.</td>
</tr>
<tr>
<td>MVR Current Multicast groups</td>
<td>The current number of MVR groups allocated.</td>
</tr>
<tr>
<td>MVR Query Response Time</td>
<td>The current MVR query response time.</td>
</tr>
<tr>
<td>MVR Mode</td>
<td>The current MVR mode. It can be compatible or dynamic.</td>
</tr>
</tbody>
</table>
The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Group IP</td>
<td>MVR group multicast IP address.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the specific MVR group. It can be active or inactive.</td>
</tr>
<tr>
<td>Members</td>
<td>The list of ports which participates in the specific MVR group.</td>
</tr>
</tbody>
</table>

**Examples**

console#show mvr members
MVR Group IP  Status  Members
----------------  --------  ---------------------
224.1.1.1        INACTIVE Gi1/0/1, Gi1/0/2, Gi1/0/3

console#show mvr members 224.1.1.1
MVR Group IP  Status  Members
----------------  --------  ---------------------
224.1.1.1        INACTIVE Gi1/0/1, Gi1/0/2, Gi1/0/3

**show mvr interface**

Use the `show mvr interface` command to display the MVR enabled interfaces configuration.

**Syntax**

`show mvr interface [interface-id [members [vlan vlan-id]]]`

- interface-id—Identifies a specific interface.
- vlan-id—VLAN identifier.

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>None</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>MVR disabled</td>
</tr>
</tbody>
</table>

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Interface number</td>
</tr>
<tr>
<td>Type</td>
<td>The MVR port type. It can be None, Receiver, or Source type.</td>
</tr>
<tr>
<td>Status</td>
<td>The interface status. It consists of two characteristics:</td>
</tr>
<tr>
<td></td>
<td>1 active or inactive indicating if port is forwarding.</td>
</tr>
<tr>
<td></td>
<td>2 inVLAN or notInVLAN indicating if the port is part of any VLAN</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>The state of immediate mode. It can be enabled or disabled.</td>
</tr>
</tbody>
</table>

**Examples**

```
console#show mvr interface
Port        Type              Status                 Immediate Leave
---------   ---------------   ---------------------  --------------------
Gi1/0/9     RECEIVER          ACTIVE/inVLAN          DISABLED

console#show mvr interface gi1/0/9
Type: RECEIVER Status: ACTIVE   Immediate Leave: DISABLED

console#show mvr interface gi1/0/23 members
235.0.0.1 STATIC   ACTIVE
```
show mvr traffic

Use the show mvr traffic command to display global MVR statistics.

Syntax

show mvr traffic

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>None</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>MVR disabled</td>
</tr>
</tbody>
</table>

Examples

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Query Received</td>
<td>Number of received IGMP Queries.</td>
</tr>
<tr>
<td>IGMP Report V1 Received</td>
<td>Number of received IGMP Reports V1.</td>
</tr>
<tr>
<td>IGMP Report V2 Received</td>
<td>Number of received IGMP Reports V2.</td>
</tr>
<tr>
<td>IGMP Leave Received</td>
<td>Number of received IGMP Leaves.</td>
</tr>
<tr>
<td>IGMP Query Transmitted</td>
<td>Number of transmitted IGMP Queries.</td>
</tr>
<tr>
<td>IGMP Report V1 Transmitted</td>
<td>Number of transmitted IGMP Reports V1.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>IGMP Report V2 Transmitted</td>
<td>Number of transmitted IGMP Reports V2.</td>
</tr>
<tr>
<td>IGMP Leave Transmitted</td>
<td>Number of transmitted IGMP Leaves.</td>
</tr>
<tr>
<td>IGMP Packet Receive Failures</td>
<td>Number of failures on receiving the IGMP packets.</td>
</tr>
<tr>
<td>IGMP Packet Transmit Failures</td>
<td>Number of failures on transmitting the IGMP packets.</td>
</tr>
</tbody>
</table>

console#show mvr traffic

IGMP Query Received......................... 2
IGMP Report V1 Received..................... 0
IGMP Report V2 Received..................... 3
IGMP Leave Received.......................... 0
IGMP Query Transmitted...................... 2
IGMP Report V1 Transmitted............... 0
IGMP Report V2 Transmitted............... 3
IGMP Leave Transmitted.................... 1
IGMP Packet Receive Failures............ 0
IGMP Packet Transmit Failures......... 0
A port channel is a set of one or more links that can be aggregated together to form a bonded channel (Link Aggregation Group or LAG or port channel). Individual conversations in a particular direction always travel over a single link in the port channel, however, in aggregate, the bandwidth usage of all of the links is fairly evenly distributed. Port channels have the advantage of allowing incremental bandwidth to be added as needed (by adding additional links) and supporting a form of fault tolerance (traffic on failed links is redistributed among other links in the LAG). LAGs are formed from similarly configured physical links, i.e. the speed, duplex, auto-negotiation, PFC configuration, DCBX configuration, etc. must be compatible on all member links. Per IEEE 802.1AX, only links with the same operational characteristics, such as speed and duplex setting, may be aggregated. Dell EMC Networking switches aggregate links only if they have the same operational speed and duplex setting, as opposed to the configured speed and duplex setting. This allows operators to aggregate links that use auto negotiation to set values for speed and duplex or to aggregate ports with SFP+ technology operating at a lower speeds, e.g., 1G. Dissimilar ports will not become active in the LAG if their operational settings do not match those of the first member of the LAG.

In practice, some ports in a LAG may auto-negotiate a different operational speed than other ports depending on the far end settings and any link impairments. Per the above, these ports will not become active members of the LAG. On a reboot or on flapping the LAG links, a lower speed port may be the first port selected to be aggregated into the LAG. In this case, the higher speed ports are not aggregated. Use the `lacp port-priority` command to select one or more primary link to lead the formation of the aggregation group.

While it is a requirement of a LAG that the link members operate at the same duplex and speed settings, administrators should be aware that copper ports have larger latencies than fiber ports. If fiber and copper ports are aggregated together, packets sent over the fiber ports may arrive significantly sooner at the destination than packets sent over the copper ports. This can cause significant issues in the receiving host (e.g. a TCP receiver) as it would be required to buffer a potentially large number of out-of-order frames. Devices
unable to buffer the requisite number of frames will show excessive frame discard. Configuring copper and fiber ports together in an aggregation group is not recommended.

If a dynamic LAG member sees an LACPDU that contains information different from the currently configured default partner values, that particular member drops out of the LAG. This configured member does not aggregate with the LAG until all the other active members see the new information. When each of the other active members sees the new information, they continue to drop out of the LAG. When all the members have dropped out of the LAG, they form an aggregate with the new information.

**Static LAGS**

A static LAG is fundamentally no different from a dynamically configured LAG. All the requirements for the member ports hold true (member ports must have same duplex settings, same speed, and so on). The only difference is this LAG has an additional parameter `static` which makes this LAG not require a partner system running Link Aggregation Control Protocol (LACP) to be able to aggregate it's member ports.

Care must be taken while enabling this type of configuration. If the Partner System is not 802.3AD compliant or the Link Aggregation Control protocol is not enabled, there may be network instability. Network instability occurs when one side assumes that the members in an aggregation are one single link, while the other side is oblivious to this aggregation and continues to treat the 'members' as individual links.

A static LAG does not transmit or process received LACPDUs, that is, the member ports do not transmit LACPDUs and all the LACPDUs it receives are dropped. A dropped counter is maintained to count the number of such PDUs.

Configured members are added to the LAG (active participation) immediately if the LAG is configured to be static. There is no wait time before we add the port to the LAG.

A LAG can be either static or dynamic, but not both. It cannot have some member ports participate in the protocol while other member ports do not participate. Additionally, it is not possible to change a LAG from static to dynamic via the CLI. You must remove the member ports from the static LAG and then add them to the dynamic LAG.
VLANs and LAGs

When Ethernet interfaces are added to a LAG, they are removed from all existing VLAN membership and take on the VLAN membership of the LAG. When members are removed from a LAG, the members regain the Ethernet interface VLAN membership as per the configuration.

LAG Thresholds

In many implementations, a LAG is declared as up if any one of its member ports is active. This enhancement provides configurability for the minimum number of member links to be active to declare a LAG up. Network administrators can also utilize this feature to automatically declare a LAG down when only some of the links have failed.

LAG Hashing

The purpose of link aggregation is to increase bandwidth between two switches. It is achieved by aggregating multiple ports in one logical group. A common problem of port channels is the possibility of changing packets order in a particular TCP session. The resolution of this problem is correct selection of an Ethernet port within the port channel for transmitting the packet to keep the original packet order.

The hashing algorithm is configurable for each LAG. Typically, an administrator is able to choose from hash algorithms utilizing the following attributes of a packet to determine the outgoing port:

- Source MAC, VLAN, EtherType, and incoming port associated with the packet.
- Source IP and Source TCP/UDP fields of the packet.
- Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- Source MAC, Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- Destination IP and Destination TCP/UDP Port fields of the packet.
- Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
• Source/Destination IP and source/destination TCP/UDP Port fields of the packet.

Enhanced LAG Hashing

Dell EMC Networking devices based on Broadcom XGS-IV silicon support configuration of hashing algorithms for each LAG interface. The hashing algorithm is used to distribute traffic load among the physical ports of the LAG while preserving the per-flow packet order.

**NOTE:** Enhanced hashing mode is not supported on the N1100-ON/N1500 Series switches.

One limitation with earlier LAG hashing techniques is that the packet attributes were fixed for all type of packets. Also, there was no MODULO-N operation involved, which can result in poor load balancing performance.

The LAG hashing support supports an enhanced hashing mode, which has the following advantages:

• MODULO-N operation based on the number of ports in the LAG.
• Packet attributes selection based on the packet type. For L2 packets, Source and Destination MAC address are used for hash computation. For IP packets, Source IP, Destination IP address, TCP/UDP ports are used.
• Non-Unicast traffic and Unicast traffic is hashed using a common hash algorithm.
• Excellent load balancing performance.
• Enhanced LAG hashing is the default hashing mode for LAGs on switches that support it.

Manual Aggregation of LAGs

Dell EMC Networking switching supports the manual addition and deletion of links to aggregates.

In the manual configuration of aggregates, the ports send their Actor Information (LACPDU) to the partner system in order to find a suitable Partner to form an aggregation. When the Partner System neglects to respond using LACPDU, the Dell EMC Networking switching aggregates manually. The Dell EMC Networking switching uses the currently configured default Partner Values for Partner Information.
Flexible Assignment of Ports to LAGs

Assignment of interfaces to dynamic LAGs is based upon a maximum of 144 interfaces assigned to dynamic LAGs, a maximum of 128 dynamic LAGs and a maximum of 8 interfaces per dynamic LAG. For example, 128 LAGs may be assigned 2 interfaces each or 18 LAGs may be assigned 8 interfaces each.

NOTE: The N1100-ON/N1500 Series switches support 64 port channels.

Commands in this Section

This section explains the following commands:

- `channel-group`
- `feature vpc`
- `interface range port-channel`
- `hashing-mode`
- `lacp port-priority`
- `lacp system-priority`
- `lacp timeout`
- `port-channel local-preference`
- `port-channel min-links`
- `show interfaces port-channel`
- `show lacp`
- `show statistics port-channel`

channel-group

Use the `channel-group` command in Interface (Ethernet) Configuration mode to associate a port with a port channel. To remove the channel-group configuration from the interface, use the `no` form of this command.

Syntax

```
channel-group port-channel-number mode {on | active}
```

```
no channel-group
```

- port-channel-number — Number of a valid port-channel with which to associate the current interface.
- on — Forces the port to join a channel without LACP (static LAG).
- active — Forces the port to join a channel with LACP (dynamic LAG).
Default Configuration
This command has no default configuration.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
This command has no user guidelines.

Example
The following example shows how port gi1/0/5 is configured in port-channel 1 without LACP (static LAG).

console(config)# interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)# channel-group 1 mode on

The following example shows how port gi1/0/6 is configured to port-channel 2 with LACP (dynamic LAG).

console(config)# interface gigabitethernet 1/0/6
console(config-if-Gi1/0/6)# channel-group 2 mode active

interface port-channel
Use the interface port-channel command in Global Configuration mode to enter port-channel configuration mode.

Syntax
interface port-channel port-channel-number

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode
**User Guidelines**

Port channel numbers range from 1 to 128 for all switches except the N1500 which supports 64 port channels.

**Example**

The following example enters the context of port-channel 1.

```
console(config)# interface port-channel 1
console(config-if-po1)#
```

**interface range port-channel**

Use the `interface range port-channel` command in Global Configuration mode to execute a command on multiple port channels at the same time.

**Syntax**

```
interface range port-channel {port-channel-range | all}
```

- `port-channel-range` — List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels. (Range: valid port-channel)
- `all` — All the channel-ports.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

Commands in the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it stops the execution of the command on subsequent interfaces.

**Example**

The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.
hashing-mode

Use the hashing-mode command to set the hashing algorithm on trunk ports. Use the no hashing-mode command to set the hashing algorithm on trunk ports to the default.

Syntax

hashing-mode mode

- mode — Mode value in the range of 1 to 7.

Range: 1–7:
- 1 — Source MAC, VLAN, EtherType, source module, and port ID
- 2 — Destination MAC, VLAN, EtherType, source module, and port ID
- 3 — Source IP and source TCP/UDP port
- 4 — Destination IP and destination TCP/UDP port
- 5 — Source/destination MAC, VLAN, EtherType, and source MODID/port
- 6 — Source/destination IP and source/destination TCP/UDP port
- 7 — Enhanced hashing mode. This mode is not available on Dell EMC Networking N1100-ON/N1500 Series switches.

Default Configuration

The default hashing mode is 7—Enhanced hashing mode. On Dell EMC Networking N1100-ON/N1500 Series switches, the default hashing mode is 5.

Command Mode

Interface Configuration (port-channel) mode
**User Guidelines**

Enhanced hashing mode is recommended, however, depending on the specific traffic patterns present in the network, a different hashing mode may give better bandwidth distribution across the LAG member links. Use the `show interfaces utilization` command to view link utilization.

**Example**

```
console(config)#interface port-channel 1
console(config-if-po1)#hashing-mode 4
console(config-if-po1)#no hashing mode
```

**l lacp port-priority**

Use the `lacp port-priority` command to configure the priority value for physical ports. To reset to default priority value, use the `no` form of this command.

**Syntax**

```
lacp port-priority value
no lacp port-priority
```

- **value** — Port priority value. (Range: 1–65535)

**Default Configuration**

The default port priority value is 1.

**Command Mode**

Interface Configuration (Ethernet) mode

Interface Range mode

**User Guidelines**

Per IEEE 802.1AX-2008 Section 5.6, ports are selected for aggregation by each switch based upon the port priority assigned by the switch with the higher system priority, starting with the highest priority port of the switch with the higher switch priority, and working downward through the ordered list of port priority values for the ports.
The port priority of each port is a four octet binary number, formed by using the configured port priority as the two most significant octets and the port number as the two least significant octets. For any given set of ports, the port with the numerically lower value of port priority has the higher priority.

The selection algorithm is reapplied upon changes in the membership of the port channel (for example, if a link fails, or if a new link joins the group) and any subsequent changes to the set of active links are made according to the above algorithm.

**Example**

The following example configures the priority value for port 1/0/8 to 247.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#lacp port-priority 247
```

**lacp system-priority**

Use the `lacp system-priority` command in Global Configuration mode to configure the Link Aggregation system priority. To reset to default, use the `no` form of this command.

**Syntax**

```
lacp system-priority value
no lacp system-priority
```

- **value** — System priority value. (Range: 1–65535)

**Default Configuration**

The default system priority value is 1.

**Command Mode**

Global Configuration mode
**User Guidelines**

Per IEEE 802.1AX-2008 Section 5.6, ports are selected for aggregation by each switch based upon the port priority assigned by the switch with the higher system priority, starting with the highest priority port of the switch with the higher switch priority, and working downward through the ordered list of port priority values for the ports.

The system priority of each switch is an eight octet binary number, formed by using the configured system priority as the two most significant octets and the switch id (MAC address) as the least significant six octets. For a given switch and link aggregation partner, the switch with the numerically lower value of system priority has the higher priority.

The selection algorithm is reapplied upon changes in the membership of the port channel (for example, if a link fails, or if a new link joins the group) and any subsequent changes to the set of active links are made according to the above algorithm.

**Example**

The following example configures the system priority to 120.

```
console(config)#lacp system-priority 120
```

**lacp timeout**

Use the `lacp timeout` command to assign an administrative LACP timeout. To reset the administrative LACP timeout to the default, use the `no` form of this command.

**Syntax**

```
lacp timeout {long | short}
no lacp timeout
```

- `long` — Specifies a long timeout value.
- `short` — Specifies a short timeout value.

**Default Configuration**

The default port timeout value is `long`. 
**Command Mode**
Interface Configuration (Ethernet) mode  
Interface Range mode

**User Guidelines**
The LACP time-out setting indicates a local preference for the rate of LACPDU transmission and the period of time before invalidating received LACPDU information. This setting is negotiated with the link partner. Long time-outs are 90 seconds with a transmission rate of once every 30 seconds. Short time-outs are 3 seconds with a transmission rate of once every second. For further information, refer to the LACP_Timeout setting in IEEE Std. 802.1AX-2008.

**Example**
The following example assigns an administrative LACP timeout for port Gi1/0/8 to a long timeout value.
```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#lacp timeout long
```

**port-channel local-preference**
Use the `port-channel local-preference` command in Interface Configuration mode to enable the local-preference mode on a port-channel (LAG) interface or range of port-channel interfaces.

Use the `no` form of the command to remove the local preference.

**Syntax**
- `port-channel local-preference`
- `no port-channel local-preference`

**Default Configuration**
By default, port channels are not configured with local preference.

**Command Mode**
Interface Configuration (port-channel) mode
User Guidelines

For a LAG that contains links distributed across stacking units, the default behavior is to distribute locally received ingress traffic across all LAG links in the stack per the selected hashing algorithm. When enabled, this command disables forwarding of ingress unicast traffic across stacking links for a LAG that is comprised of links on multiple stack units. It does this by restricting LAG hashing to only select egress links on the stack unit where the traffic ingresses.

⚠️ CAUTION: If the capacity of the local egress LAG links is exceeded, traffic will be discarded. Therefore, use of this option should be carefully considered, and the operator must ensure that sufficient egress bandwidth is available in the LAG links on every stack member to avoid excessive discards.

By default, the local-preference mode for a port-channel is disabled. This command can be used only on port-channel interfaces.

Example

```
console(config)#interface port-channel 1
console(config-if-Po1)#port-channel local-preference
console(config-if-Po1)#no port-channel local-preference
```

Command History

Example added in the 6.4 release.

port-channel min-links

Use the `port-channel min-links` command in Interface Configuration (port-channel) mode to set the minimum number of links that must be up in order for the port channel interface to be declared up. Use the `no` form of the command to return the configuration to the default value (1).

Syntax

```
port-channel min-links <1-8>
no port-channel min-links
```

- **min-links**—The minimum number of links that must be active before the link is declared up. Range 1-8. The default is 1.
Default Configuration
The default minimum links is 1.

Command Mode
Interface Configuration (port-channel) mode

User Guidelines
This command has no user guidelines.

Example
console(config)#interface port-channel 1
console(config-if-Po1)#port-channel min-links 3
console(config-if-Po1)#no port-channel min-links

show interfaces port-channel
Use the show interfaces port-channel command to show port-channel information.

Syntax
show interfaces port-channel [port-channel-number]

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
The command displays the following information.
Example #1

console#show interfaces port-channel 1

<table>
<thead>
<tr>
<th>Channel</th>
<th>Ports</th>
<th>Ch-Type</th>
<th>Hash Type</th>
<th>Min-links</th>
<th>Local Prf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Po1</td>
<td>Inactive: Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4</td>
<td>Dynamic</td>
<td>3</td>
<td>1</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Hash Algorithm Type
1 - Source MAC, VLAN, EtherType, source module and port ID
2 - Destination MAC, VLAN, EtherType, source module and port ID
3 - Source IP and source TCP/UDP port
4 - Destination IP and destination TCP/UDP port
5 - Source/Destination MAC, VLAN, EtherType, source MODID/port
6 - Source/Destination IP and source/destination TCP/UDP port
7 - Enhanced hashing mode

**show lacp**

Use this command to display LACP information for Ethernet ports.

**Syntax**

```
show lacp {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}[parameters | statistics]
```
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example shows how to display LACP Ethernet interface information.

console#show lacp gi1/0/1

port Gi1/0/1 LACP parameters:
Actor:
  system priority: 1
  port Admin key: 0
  port oper key: 1
  port oper priority: 1
  port oper timeout: LONG
  port Admin timeout: LONG
  LACP Activity: ACTIVE
  Aggregation: AGGREGATABLE
  synchronization: FALSE
  collecting: FALSE
  distributing: FALSE
  expired: FALSE
Partner:
  port Admin key: 0
  port oper key: 0
  port Admin priority: 0
  port oper priority: 0
  port Oper timeout: LONG
  LACP Activity: PASSIVE
  Aggregation: NOTAGGREGATABLE
  synchronization: FALSE
  collecting: FALSE
  distributing: FALSE
  expired: FALSE

port Gi1/0/1 LACP Statistics:
Layer 2 Switching Commands

show statistics port-channel

Use the show statistics port-channel command to display statistics about a specific port-channel.

Syntax

show statistics port-channel port-channel-number

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example shows statistics about port-channel 1.

```
console#show statistics port-channel 1

Total Packets Received (Octets)................ 0
Packets Received 64 Octets..................... 0
Packets Received 65-127 Octets................. 0
Packets Received 128-255 Octets.............. 0
Packets Received 256-511 Octets.............. 0
Packets Received 512-1023 Octets............. 0
Packets Received 1024-1518 Octets............ 0
Packets Received > 1518 Octets............... 0
Packets RX and TX 64 Octets.................. 0
Packets RX and TX 65-127 Octets.............. 0
Packets RX and TX 128-255 Octets............ 0
Packets RX and TX 256-511 Octets............ 0
Packets RX and TX 512-1023 Octets........... 0
Packets RX and TX 1024-1518 Octets.......... 0
Packets RX and TX 1519-2047 Octets.......... 0
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets RX and TX 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets RX and TX 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Received Without Errors</td>
<td>0</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>0</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>0</td>
</tr>
<tr>
<td>Receive Packets Discarded</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Received with MAC Errors</td>
<td>0</td>
</tr>
<tr>
<td>Jabbers Received</td>
<td>0</td>
</tr>
<tr>
<td>Fragments/Undersize Received</td>
<td>0</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>0</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>Overruns</td>
<td>0</td>
</tr>
<tr>
<td>Total Received Packets Not Forwarded</td>
<td>0</td>
</tr>
<tr>
<td>802.3x Pause Frames Received</td>
<td>0</td>
</tr>
<tr>
<td>Unacceptable Frame Type</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Transmitted (Octets)</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 64 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 65-127 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 128-255 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 256-511 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 512-1023 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted 1024-1518 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Packets Transmitted &gt; 1518 Octets</td>
<td>0</td>
</tr>
<tr>
<td>Max Frame Size</td>
<td>1518</td>
</tr>
<tr>
<td>Total Packets Transmitted Successfully</td>
<td>0</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>0</td>
</tr>
<tr>
<td>Multicast Packets Transmitted</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>0</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>0</td>
</tr>
<tr>
<td>Total Transmit Errors</td>
<td>0</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>Underrun Errors</td>
<td>0</td>
</tr>
<tr>
<td>Total Transmit Packets Discarded</td>
<td>0</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>0</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>0</td>
</tr>
<tr>
<td>Excessive Collision Frames</td>
<td>0</td>
</tr>
<tr>
<td>802.3x Pause Frames Transmitted</td>
<td>0</td>
</tr>
<tr>
<td>GVRP PDUs received</td>
<td>0</td>
</tr>
</tbody>
</table>
GVRP PDUs Transmitted.......................... 0
GVRP Failed Registrations...................... 0
GMRF PDUs Received.............................. 0
GMRF PDUs Transmitted.......................... 0
GMRF Failed Registrations...................... 0
BPDUs: Sent: 0, Received: 0

Time since counters last cleared.............. 0 day 6 hr 19 min 42 sec
Port Monitor Commands

**Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches**

Dell EMC Networking switches allow the user to monitor traffic with an external network analyzer. The external network analyzer can use any of the Ethernet ports as a probe port. The probe port transmits a mirror copy of the traffic being probed. Network traffic transmission is always disrupted whenever a configuration change is made for port monitoring. Therefore, whenever port monitoring is enabled, the probe port does not always forward traffic as a normal port. When diagnosing problems, an operator should always check the status of port monitoring.

The port monitoring feature allows the user to configure a session. A session consists of one destination or probe port and one or multiple source ports. When a session is enabled, any traffic entering or leaving the source ports of that session is copied (mirrored) onto the corresponding destination port. A network traffic analyzer can be attached to destination ports to analyze the traffic patterns of source ports.

A session is operationally active only if both a destination port and at least one source port are configured. If neither is true, the session is inactive. A port configured as a destination port acts as a mirroring port when the session is operationally active. If it is not, the port acts as a normal port and participates in all normal operation with respect to transmitting traffic.

The port mirroring logic stage occurs after the after the VLAN tag processing stage on ingress and before the VLAN tag processing stage on egress. When mirroring packets associated with DVLAN/QinQ SP or CE ports, the outer VLAN tag may or may not appear in the frame. Due to the internal processing of QinQ tagging, the TPID of ingress frames mirrored from the SP port will always be 0x8100. In addition, packets forwarded internally across a stacking link may have different tags applied than packets forwarded on a local egress port. This is due to the processing required for forwarding across a stack.

Any Ethernet port may be configured as a source port.

**Caveats:**

- Platforms may behave unpredictably if an attempt is made to mirror a port of greater speed than the probe port.
Once configured, there is no network connectivity on the probe (destination) port. The probe port does not forward any traffic and does not receive any traffic. The probe tool attached to the probe port is unable to ping the networking device or ping through the networking device, and no device is able to ping the probe tool.

ACL attributes redirect, mirror, log, rate-limit, assign-queue, time-range, IGMP type, ICMP type, ICMP code, routing, fragments, and TCP established are not supported when applied to a mirroring session.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture (Global Configuration)</td>
<td>remote-span</td>
</tr>
<tr>
<td>monitor capture (Privileged Exec)</td>
<td>show monitor capture</td>
</tr>
<tr>
<td>monitor capture mode</td>
<td>show monitor session</td>
</tr>
<tr>
<td>monitor session</td>
<td>show vlan remote-span</td>
</tr>
</tbody>
</table>

monitor capture (Global Configuration)

Use the monitor capture command to capture packets transmitted or received from the CPU. This facility captures switch control plane traffic and is useful in monitoring network control traffic and analyzing network security.

No monitor capture file size returns the capture file size to the defaults.
No monitor capture remote port returns the TCP port to the default.

Syntax

monitor capture {file size max-size | remote port id | line wrap}
no monitor capture {file size | remote port | line wrap}

- max-size—The size of the capture file in bytes.
- id—The local (switch) TCP port for use with Wireshark.

Default Configuration

Capture is not enabled by default.
The in memory buffer is 128 packets.
The file system buffer is 524288 bytes and is named cpuPktCapture.pcap.
The remote monitor capture port is 2002.

**Command Modes**

Global Configuration mode

**User Guidelines**

Packets that are transmitted or received by the switch CPU may be captured to the switch file system, to local memory, or sent to a WireShark client.
Packets captured to the switch file system are stored in pcap format and may be copied from the system and opened with WireShark or TShark or other utilities. Packets sent to the console are written in ASCII hex format.

When WireShark is configured and connected to the switch, packet capture is controlled by WireShark. See the Users Configuration Guide for an example of how to configure WireShark for packet capture.

Changes to configuration take effect on the next execution of the monitor capture start command.

Only one of file, remote, or line may be specified. Setting the file, remote, or line stops the capture.

**No monitor capture file size** returns the capture file size to the defaults

**No monitor capture remote port** returns the TCP port to the default

The administrator can capture packets into one of the following locations: memory, switch NVRAM, or directly to a Wireshark analyzer.

**Example**

Configure capture for Wireshark remote access on port 2020:

```
console(config)#monitor capture remote port 2020
console(config)#monitor capture mode remote
console(config)#exit
console#monitor capture start
```

Copy the local capture file to a TFTP server

```
console#copy flash://cpuPktCapture.pcap tftp://10.267.9.99/mypkts.pcap
```
monitor capture (Privileged Exec)

Use the `monitor capture` command to capture packets transmitted or received from the CPU. This facility captures switch control plane traffic and is useful in monitoring network control traffic and analyzing network security. Remote packet capture is not supported when the packets are received via Service Port.

**Syntax**

```
monitor capture {start [transmit | receive | all] | stop}
```

- **Transmit**—Capture packets transmitted by the switch CPU.
- **Receive**—Capture packets forwarded to the switch CPU.
- **All**—Capture both transmitted and received packets.

**Default Configuration**

Capture is not enabled by default.
By default, both transmitted and received packets are captured.

**Command Modes**

Privileged Exec mode

**User Guidelines**

In general, starting packet capture erases the previous capture buffer contents.

**Example**

```
console# monitor capture start all
```

**monitor capture mode**

Use the `monitor capture mode` command to select the destination for captured packets transmitted or received from the CPU. This facility captures switch control plane traffic and is useful in monitoring network control traffic and analyzing network security.

Use the `no` form of the command to return the capture mode to the default.
**Syntax**

```
monitor capture mode {line | remote | file}
no monitor capture mode
```

- **line**—Captured packets are sent to the console.
- **remote**—Captured packets are sent to a remote WireShark network analyzer.
- **file**—Captured packets are sent to the file system.

**Default Configuration**

By default, remote capture is configured.

**Command Modes**

Global Configuration mode

**User Guidelines**

Only one file, remote, or line may be specified. Setting the mode takes effect immediately.

Use the `monitor capture start` command to start the capture.

**Memory Capture:**

Captured packets can be displayed on the console using the `show monitor capture packets` command. Captured packets can be displayed when actively capturing or when stopped. When a capture session is active, it is possible to display only the captured packets which were not previously displayed as the show command empties the capture buffer. When a capture session is stopped, it is possible to display all saved packets as often as required. The command `show monitor capture packets` always displays the captured packets in chronological order.

The memory buffer only stores the first 128 bytes of each packet captured.

The switch displays the following information from the captured packet when it is displayed on CLI:

- Packet is transmitted or received.
- ID of interface through which the packet was passed.
- The time when packet passed through CPU.
- The first 128 bytes of packet.
- The length of full packet (if greater than 128 bytes).

The in-memory capture buffer can be configured to stop when full. This mode is configured with the command `no monitor capture line wrap`. Capturing packets is started by the `monitor capture start` command. Capturing packets is stopped automatically when 128 packets are captured and saved into the RAM. Capturing packets can be stopped manually before 128 packets have been captured using the `monitor capture stop` command to halt packet capture.

If capturing is in progress, the `show monitor capture packets` command displays only captured packets that have not yet been displayed during capturing session. If capturing is stopped, the first (after stopping) `show monitor capture packets` command displays packets which have not yet been displayed during capturing session. The next `show monitor capture packets` command displays all saved packets.

If the capturing session is stopped automatically during the period packet display is in progress, the packets display continues until all saved packets are shown and then the buffer is cleared. The next invocation of the `show capture packets` command will not display any packets. Please note that this behavior is observed only if the capturing session is stopped automatically when the packet displaying is in progress.

The in-memory capture can also be configured to wrap. This makes it possible to display more than 128 packets per capture session if the command `show capture packets` is periodically executed while capture is in progress. Saved packets that have been already displayed during the capturing session are overwritten in RAM by new captured packets if capturing is still in progress. In this manner, the limit of displaying 128 packets per session can be overcome (but only in `monitor capture line wrap` mode). Packets that have not been displayed are not overwritten.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during capturing session. It is guaranteed that no one packet will be lost (not be displayed or not be saved) when capturing is in progress. In this case, the last 128 packets are saved into the RAM and can be displayed many number of times by executing the command `show monitor capture packets`. 
If capturing is in progress and more than 128 packets are captured and the user configures **no monitor capture line wrap** mode, capturing is stopped automatically. No packets are lost when capturing is in progress.

All captured packets can be displayed. No captured and not yet displayed packets are lost. Captured packets can be displayed when capturing is in progress or after the moment when capturing is stopped. Only packets saved in RAM (up to 128) can be displayed when capturing is stopped.

If capturing is in progress, the **show monitor capture packets** command displays only the captured packets that have not yet been displayed during the capturing session. If capturing is stopped, the first (after stopping) **show monitor capture packets** command displays the packets that have not yet been displayed during the capturing session. The next **show monitor capture packets** command displays up to 128 captured packets.

If the capturing session is stopped automatically when the packet display is in progress, then packet display continues until all packets are shown. The next call of the **show capture packets** command displays nothing. Please note that such behavior is observed only if the capturing session is stopped automatically when the packet display is in progress.

**NVRAM Capture:**

After packet capture is activated, packets are stored in NVRAM until the capture file reaches its maximum size, or until the capture is stopped manually. When the capture is started the capture file from the previous capture is deleted.

The captured file can be uploaded via TFTP, SFTP, SCP via CLI, and SNMP using the **copy** command. The name of the capture file is cpuPktCapture.pcap.

**Remote Capture:**

Remote Packet Capture works with the Wireshark network analyzer tool. A packet capture server runs on the switch and sends the captured packets via a TCP connection to the Wireshark tool. Once a connection is established, packet capture is started and stopped via Wireshark commands.
Remote capture can be enabled or disabled using the CLI. The network operator should obtain a computer with the Wireshark tool to display the captured traffic. When using remote capture mode, the switch doesn’t store any captured data locally.

The local TCP port number can be configured for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, these ports must be allowed to pass through the firewall. The Firewall must be configured to allow the Wireshark PC to initiate a TCP connection to the switch.

The remote capture application listens on the configured TCP port for a connection request. Wireshark must send a request to that port to establish a connection. Once the socket connection to Wireshark has been established, captured CPU packets are written to the data socket. Wireshark receives the packets and processes them locally. This continues until the session is terminated by either end.

The following Wireshark request packets are supported:

- Request to list all the remote interfaces
- Request to open a remote device
- Request to start a capture on a remote device
- Request to close the connection with the remote peer
- Message that keeps the authentication parameters
- Request to get network statistics
- Request to stop the current capture, keeping the device open

The following Wireshark replies are supported:

- Reply that sends the list of all the remote interfaces
- Reply that the remote device has been opened correctly
- Reply that capturing has started correctly
- Reply that says 'ok, authorization successful'
- Reply that keeps network statistics
- Reply that confirms capturing stopped successfully

Remote capture is not supported for packets received via out-of-band ports.
Example

This example sends capture output to the console.

```console
console(config)#monitor capture line
console(config)#exit
console#monitor capture start all
```

**monitor session**

Use the **monitor session** command in Global Configuration mode to configure the source and destination for mirroring. Packets are copied from the source to the destination. Use the **no** form of the command to disable the monitoring session.

**Syntax**

```plaintext
monitor session session-number source {interface interface–id | vlan vlan-id | remote vlan rspan-vlan-id} [rx | tx]
no monitor session session_number source {interface interface–id | vlan vlan-id | remote vlan rspan-vlan-id}

[no] monitor session session_number destination {interface interface–id [remove-rspan-tag] | remote vlan rspan-vlan-id}

[no] monitor session session_number filter {ip access-group [acl-name | acl-number] | mac access-group acl-name}

no monitor session session_number mode
```

**no monitor session session_number mode**

- **session-number**— Session identification number. (Range: 1-4)
- **interface interface–id** — Ethernet interface (Range: Any valid Ethernet Port), CPU interface. CPU interface is not supported as a destination interface or a source interface for RSPAN.
- **vlan vlan-id**— The source VLAN identifier. All the ports in this VLAN are mirrored in the ingress direction only. The source VLAN must not be the RSPAN VLAN.
- **acl-name**— An IP or MAC ACL name.
- **remote vlan rspan-vlan-id**— An RSPAN VLAN configured on the source switch.
- **rx** — Mirrors received packets only. If no option specified, monitors both rx and tx.
- **tx** — Mirrors transmitted packets only. If no option is specified, monitors both rx and tx.
- **both**—Mirrors both ingress and egress. This is the default.
- **mode**—Enable session mirroring. Use the no form of the command to disable monitoring.
- **remove-rspan-tag**—Remove the RSPAN tag from packets transmitted on the probe port. This option is not available on the N4000 Series switches.

**Default Configuration**
The default is to mirror both transmit and receive directions. If neither tx or rx is configured, both directions are monitored.

**Command Mode**
Global Configuration mode

**User Guidelines**
Use the source interlace parameter to specify the interface to monitor. Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an rx or tx option, the session monitors both ingress and egress packets. Use the destination interface to specify the interface to receive the monitored traffic. Use the mode parameter to enabled the administrative mode of the session. If enabled, the destination (probe) port monitors all the traffic received and transmitted on the physical monitored port. The probe port should not be connected to a network. Connect it to a monitoring tool or a standalone (static IP address) workstation running a monitoring program.

Up to four sessions mirroring traffic in a single direction and with unique destinations are supported on the Dell EMC Networking N2000, N2100-ON, N3000, N3100-ON, and N4000 Series switches. The Dell EMC Networking N1100-ON and N1500 Series switches support a single unidirectional or bidirectional session. Each session supports multiple sources. However, the destination interface for a session may not overlap with other sessions. The internal CPU port cannot be configured as an RSPAN source.

The session limitations are as follows (N2000, N2100-ON, N3000, N3100-ON, N4000 only):
- Up to 4 sessions in ingress (RX) traffic mirroring may be active.
• Up to 4 sessions with egress (TX) traffic mirroring may be active.
• Up to 2 sessions with both (RX and TX) traffic mirroring may be active.
• Any other combination of up to 4 total ingress or egress mirroring may be active.

Destination (probe) interfaces do not perform MAC learning and drop ingress traffic (forwarding is disabled and incoming packets are dropped). Routing, spanning-tree, and port channel configuration are operationally disabled on probe ports. Destination interfaces must be dedicated to the monitoring function (i.e., connected to a PC running WireShark or some other packet decoder).

VLAN based mirroring is applicable only for ingress (RX) traffic. If neither rx, tx, nor both are specified in a source session, both ingress and egress traffic are monitored.

Mirrored traffic is subject to the same QoS constraints as normal traffic. Oversubscribed traffic (both mirrored and un-mirrored) will be dropped in accordance with the configured or default policy. The operator may assign CoS or Diffserv policies to the mirrored traffic in the same manner as for normal traffic. RSPAN traffic is transmitted with a PCP of 0.

On ingress, the port mirroring logic stage is after the VLAN tag processing stage in the hardware. This means that, on ingress, packets may not appear as they do on the wire if processing such as VLAN or CoS value rewriting is programmed or DVLAN tunneling is enabled on the source interface. Examples of ingress VLAN tag processing are DVLAN tunneling (QinQ) or VLAN rewriting. Likewise, on egress, the port mirroring logic stage is before the egress VLAN tag processing stage. This means that, on egress, packets may not appear as they do on the wire if processing such as VLAN or CoS value rewriting is programmed.

Reserve a few VLANs across the network for the exclusive use of RSPAN. The RSPAN VLANs should only be configured on the reflector interfaces (generally the uplink/transit/downlink interface). RSPAN VLANs are used exclusively to carry the mirrored traffic across the network and cannot have source or destination interfaces as members of the RSPAN VLAN. RSPAN destination interfaces will continue to transmit mirrored traffic even if blocked by spanning-tree. Each RSPAN session must use a unique reflector port, destination port and RSPAN VLAN. Reflector ports (source/transit/destination) should be configured as trunk or general mode.
ports, and be members of the RSPAN VLAN. Do not assign other ports to the RSPAN VLANs (for example, trunk ports that are not reflector ports). Additionally, reflector ports may not be port channels.

Monitored traffic is encapsulated in the RSPAN VLAN on the reflector port on the source switch. On a source switch, when both an RSPAN VLAN and reflector port are configured on a trunk or general mode port with other VLANs, the interface can also carry traffic on the other VLANs. For example, an uplink interface (trunk port) can carry both the RSPAN traffic and other traffic. Do not configure the RSPAN VLAN as a native VLAN on interfaces other than the uplink/transit/downlink interfaces. Be sure to remove the RSPAN VLAN from ports on which mirrored traffic should not be encapsulated and transported. The RSPAN tag is not transmitted on the destination (probe) port, except on the N4000, where the RSPAN tag appears on the probe port due to hardware limitations.

For VLAN mirroring, the source VLAN cannot be the same as the RSPAN VLAN. The source VLAN and the RSPAN VLAN cannot be configured on the same port. The source VLAN is monitored in the ingress direction only. Careful consideration to placement of source mirroring sessions will allow bidirectional traffic to be monitored. Another alternative is to use port mirroring and a VLAN ACL filter if duplicate packets are received on the probe device.

The reflector port must be configured as the only member of the RSPAN VLAN on the source switch.

Multiple source interfaces may mirror traffic onto the RSPAN VLAN on both source switches and transmit switches (but not the destination switch). Be aware that the RSPAN VLAN floods mirrored traffic in the RSPAN VLAN. If an intermediate switch mirrors traffic onto the RSPAN VLAN, the traffic is flooded to both the destination and the other sources. Configuration of an ACL on the reflector port may mitigate this behavior. The source interface must be configured as the only member of the RSPAN VLAN on the destination (probe) switch. Mirroring a source to the RSPAN VLAN on the destination switch is not supported.

If an ACL filter is specified, the ACL must be created prior to its use in an RSPAN configuration. The ACL filter is configured on the source switch. ACL filters are internally configured as an egress ACL on the destination interface/reflector port. All the criteria in the ACL are marked with the mirror attribute (and the RSPAN VLAN) to match the mirrored traffic (including
the implicit deny all). If configuring an egress ACL on the destination port, care must be taken with the ACL numbering to ensure the mirrored traffic is properly processed.

Bidirectional mirroring of multiple ports in a network may result in duplicate packets transmitted on the probe port (one copy for the receive side and another copy for the transmit side). Configuring the mirroring as rx only may help to reduce this issue.

RSPAN VLANs must be configured with the remote-span command prior to configuration in an RSPAN session. RSPAN intermediate switches may also be configured with multiple sources feeding into an existing RSPAN VLAN. The source configuration requires an interface parameter, so traffic mirrored on the intermediate switch is not flooded across the entire RSPAN VLAN. Place probe ports upstream of the intermediate switch in this case.

Configuring a second session on a source switch that mirrors RSPAN traffic from the reflector port is not supported. Configuring a second session on a source switch that mirrors an RSPAN source port to a local probe port is supported.

VLAN mirroring is not recommended for RSPAN if sources on multiple switches are members of the VLAN. This is because, as stations communicate with each other over the mirrored VLAN, duplicate packets will be sent to the probe, once for the source port and once for each switch over which the packet is received in the source VLAN.

Example

This example shows how to configure a source switch using VLAN 723 as the destination RSPAN VLAN and Gi1/0/3 as the source interface. Te1/0/1 is configured as the reflector port. It is recommended that interface Te1/0/1 be configured as a trunk port. Interface Te1/0/1 must be configured as a member of VLAN 723 and may also carry traffic on other VLANs. No other interface should be configured as a member of VLAN 723.

```
console(config)#vlan 723
console(config-vlan723)#remote-span
console(config-vlan723)#exit
console(config)#interface Te1/0/1
console(config-if-Te1/0/1)#switchport mode trunk
console(config-if-Te1/0/1)#exit
console(config)#monitor session 1 source interface gi1/0/3 both
```
console(config)#monitor session 1 destination remote vlan 723 reflector-port Te1/0/1
console(config)#monitor session 1 mode
console(config)#show monitor session 1

Session : 1
Admin mode : Enabled
Type : Remote source session
Source ports :
  Both : Gi1/0/48
Destination port : Te1/0/1
Destination RSPAN VLAN : 723

This example shows how to configure a destination switch using VLAN 723 as the source RSPAN VLAN interface Te1/0/1 and Gi1/0/10 as the destination interface. Interface Gi1/0/10 is dedicated to monitoring and has a PC running WireShark attached. VLAN 723 should only be configured on interface Te1/0/1.

console(config)#vlan 723
console(config-vlan723)#remote-span
console(config-vlan723)#exit
console(config)#interface Te1/0/1
console(config-if-Tel/0/1)#switchport mode trunk
console(config-if-Tel/0/10)#exit
console(config)# monitor session 1 source remote vlan 723
console(config)# monitor session 1 destination interface gi1/0/10
console(config)# monitor session 1 mode
console(config)#show monitor session 1
Session : 1
Admin mode : Enabled
Type : Remote destination session
Source RSPAN VLAN : 723
Destination port : Gi1/0/10

**Command History**
Revised in firmware release 6.3.6.

**remote-span**
Use this command to configure a VLAN as an RSPAN VLAN. Use the `no` form of the command to remove the remote SPAN characteristics from a VLAN and revert it to a normal MAC learning VLAN.
**Syntax**

remote-span
no remote-span

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

VLAN Configuration mode.

**User Guidelines**

Remote-span VLANs must be configured as a tagged VLAN on trunk or general mode ports on RSPAN transit switches. Traffic in an RSPAN VLAN is always flooded as MAC address learning and link local protocols are disabled on RSPAN VLANs. VLANs on transit switches must be configured as remote-span VLANs in order to ensure delivery of all mirrored packets. Remote-span VLANs configured on transit switches may co-exist with other non remote-span VLANs on trunk ports. Do not configure the RSPAN VLAN as a member of spanning tree (RSTP-PV or MST).

**Example**

```
console#vlan 10
console(config-vlan10)#remote-span
```

**show monitor capture**

Use this command to display captured packets transmitted or received from the CPU.

**Syntax**

show monitor capture [packets]

**Default Configuration**

This command has no default configuration.
**Command Modes**
Privileged Exec mode (all SHOW modes)

**User Guidelines**
This command has no user guidelines.

**Example**
```
console#show monitor capture

Operational Status............................. Enabled
Current Capturing Type......................... Line
Capturing Traffic Mode.......................... Tx/Rx
Line Wrap Mode.................................. Disabled
RPCAP Listening Port........................... 2002
RPCAP dump file size (KB)...................... 45

console#show monitor capture packets

Gi1/0/1  Length = 94  [RECEIVE]
-------------
02:29:23.0000
0000 33 33 00 00 00 01 00 11 88 2f 8e 82 81 00 00 01
0010 86 dd 60 00 00 00 00 24 00 01 fe 80 00 00 00 00
0020 00 00 00 00 88 ff fe 2f 8e 82 ff 02 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 01 3a 00 05 02 00 00
0040 01 00 82 00 43 62 27 10 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 ff ff 00 00
-------------
Gi1/0/1  Length = 94  [RECEIVE]
-------------
02:29:24.0000
0000 33 33 00 00 00 01 00 11 88 2f 8e 82 81 00 00 01
0010 86 dd 60 00 00 00 00 24 00 01 fe 80 00 00 00 00
0020 00 00 00 00 88 ff fe 2f 8e 82 ff 02 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 01 3a 00 05 02 00 00
0040 01 00 82 00 43 62 27 10 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 ff ff 00 00
-------------
Gi1/0/1  Length = 94  [RECEIVE]
-------------
02:29:25.0000
0000 33 33 00 00 00 01 00 11 88 2f 8e 82 81 00 00 01
```
show monitor session

Use the **show monitor session** command to display status of port monitoring, VLAN-based mirroring, Flow-based mirroring, and mirroring across RSPAN.

**Syntax**

show monitor session session_number [detail]

- session_number—Session identification number.
- detail—Displays additional information.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

The following example shows port monitor status.
console(config)#show monitor session 1

Session : 1
Admin mode : Disabled
Type : Local session
Source ports :
  Both : Te1/0/10
Destination ports : Te2/0/20
IP access-group : a1

The following example shows the detailed status of the port based mirroring session that is constrained to a local switch.

console(config)#show monitor session 1 detail

Session : 1
Admin mode : Disabled
Type : Local session
Source ports :
  Rx only : None
  Tx only : None
  Both : Te1/0/10
Source VLANs :
  Rx only : None
Source RSPAN VLAN : None
Destination ports : Te2/0/20
Destination RSPAN VLAN : None
IP access-group : a1
MAC access-group : None

The following example shows the detailed status of a VLAN session on source switch, where session is span across multiple switches.

console# show monitor session 1 detail
Session : 1
Type : Remote Destination Session
Source Ports :
  RX Only : None
  TX Only : None
  Both : None
Source VLANs :
  Rx Only : 100
Source RSPAN VLAN : None
Destination Ports : None
Dest RSPAN VLAN : 999
The following example shows the detailed status of a VLAN session on destination switch, where session is span across multiple switches.

```
console# show monitor session 1 detail
Session           : 1
Type              : Remote Destination Session
Source Ports      :
  RX Only       : None
  TX Only       : None
  Both          : None
Source VLANs      :
  RX Only       : None
Source RSPAN VLAN : 999
Destination Ports : Gi1/0/15
Dest RSPAN VLAN   : None
```

**show vlan remote-span**

Use this command to display the RSPAN VLAN IDs.

**Syntax**

```
show vlan remote-span
```

**Default Configuration**

This command has no default configuration.

**Command Modes**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example shows the RSPAN VLANs configured on the switch.

```
console# show vlan remote-span
```

RSPAN Vlan
QoS Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Quality of Service (QoS) technologies are intended to provide guaranteed timely delivery of specific application data to a particular destination. In contrast, standard IP-based networks are designed to provide best effort data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as electronic mail and file transfer, a slight degradation in service is acceptable and, in many cases, unnoticeable.

Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. To accomplish this, all elements of the network must be QoS-capable. If one node is unable to meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

Access Control Lists

The Dell EMC Networking ACL feature allows classification of packets based upon Layer 2 through Layer 4 header information. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique Ether-type value; thus, all IPv4 and IPv6 classifiers include the Ether-type field.

Multiple ACLs per interface are supported. The ACLs can be combination of Layer 2 and/or Layer 3/4 ACLs.

ACL assignment is appropriate for both physical ports and LAGs.

A user configures an ACL permit rule to force its matching traffic stream to a specific egress interface, bypassing any forwarding decision normally performed by the device. The interface can be an Ethernet interface or a LAG. The redirect interface rule action is independent of, but compatible with, the assign queue rule action.
ACLs can be configured to apply to a VLAN instead of an interface. Traffic tagged with a VLAN ID (either receive-tagged or tagged by ingress process such as PVID) is evaluated for a match regardless of the interface on which it is received.

**Layer 2 ACLs**

The Layer 2 ACL feature provides access list capability by allowing classification on the Layer 2 header of an Ethernet frame, including the 802.1Q VLAN tag(s). In addition, the rule action set is enhanced to designate which (egress) CoS queue should handle the traffic, and whether the traffic flow is to be redirected to a specific outgoing interface.

MAC access lists are identified by a user-specified name instead of a number.

**Layer 3/4 IPv4 ACLs**

The Layer 3/4 ACL feature supports extended IP access lists. These lists check the Layer 3 portion of a packet, looking specifically at information contained in the IP header and, in certain cases, the TCP or UDP header. An EtherType of 0x0800 is assumed in the case of IP access lists. Permit and deny actions are supported for each ACL rule.

Standard layer 3/4 ACLs can be classified based on the source IP address and netmask or other extended classification criteria.

**Class of Service (CoS)**

The Dell EMC Networking CoS Queuing feature allows the user to directly configure device queuing and, therefore, provide the desired QoS behavior without the complexities of DiffServ. The CoS feature allows the user to determine the following queue behavior:

- Queue Mapping
  - Trusted Port Queue Mapping
  - Untrusted Port Default Priority
- Queue Configuration

This enables Dell EMC Networking switches to support a wide variety of delay sensitive video and audio multicast applications.
CoS mapping tables, port default priority, and hardware queue parameters may be configured on LAG interfaces as well as physical port interfaces.

**Queue Mapping**

The priority of a packet arriving at an interface is used to steer the packet to the appropriate outbound CoS queue through a mapping table. Network packets arriving at an ingress port are directed to one of n queues in an egress port(s) based on the translation of packet priority to CoS queue. The CoS mapping tables define the queue used to handle each enumerated type of user priority designated in either the 802.1p User Priority, or IP DSCP contents of a packet. If neither of these fields is trusted to contain a meaningful COS queue designation, the ingress port can be configured to use its default priority to specify the CoS queue.

CoS queue mappings use the concept of trusted and untrusted ports. A trusted port is one that takes at face value a certain priority designation within arriving packets. Specifically, a port may be configured to trust one of the following packet fields:

- IEEE 802.1p User Priority
- IP Precedence
- IP DSCP

Packets arriving at the port ingress are inspected and their trusted field value is used to designate the COS queue that the packet is placed when forwarded to the appropriate egress port. A mapping table associates the trusted field value with the desired COS queue.

Alternatively, a port may be configured as untrusted, whereby it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific COS queue on the appropriate egress port(s) in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the User Priority or IP DSCP value.
**DiffServ**

Standard IP-based networks are designed to provide “best effort” data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will meet the latency or bandwidth requirements. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Diffserv allows the network operator to classify and apply a distinguished service to traffic based on a number of criteria. The distinguished service can meter traffic and apply per hop behavior based upon the bandwidth utilization and burstiness of traffic. In addition, preferential drop characteristics can be configured in support of an assured forwarding capability such that TCP clients are informed if they exceed the switch buffering limits.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Show Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>assign-queue</td>
<td>match access-group</td>
<td>show classofservice ip-dscp-mapping</td>
</tr>
<tr>
<td>class</td>
<td>match class-map</td>
<td>show classofservice trust</td>
</tr>
<tr>
<td>class-map</td>
<td>match cos</td>
<td>show diffserv</td>
</tr>
<tr>
<td>class-map rename</td>
<td>match destination-address mac</td>
<td>show diffserv service interface</td>
</tr>
<tr>
<td>classofservice</td>
<td>match any</td>
<td>show diffserv service brief</td>
</tr>
<tr>
<td>dot1p-mapping</td>
<td>police-simple</td>
<td>show interfaces cos-queue</td>
</tr>
<tr>
<td>classofservice</td>
<td>match dstip</td>
<td>show interfaces random-detect</td>
</tr>
<tr>
<td>ip-dscp-mapping</td>
<td>police-single-rate</td>
<td></td>
</tr>
<tr>
<td>classofservice trust</td>
<td>match dstip6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>police-two-rate</td>
<td></td>
</tr>
</tbody>
</table>
Use the **assign-queue** command in Policy-Class-Map Configuration mode to modify the queue ID to which the associated traffic stream is assigned.

**Syntax**

```assign-queue queueid```

- **queueid** — Specifies a valid queue ID. (Range: integer from 0–6.)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode
**User Guidelines**

The queue id is the internal queue number (traffic class), not the CoS value. Use the `show classofservice` command to display the assignment of CoS and DSCP values to internal queue numbers.

**Example**

The following example displays how to change the queue ID to 4 for the associated traffic stream.

```
console(config-policy-classmap)#assign-queue 4
```

**class**

Use the `class` command in Policy-Map Class Configuration mode to create an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.

**Syntax**

```
class classname
no class
```

- `classname` — Specifies the name of an existing DiffServ class. (Range: 1–31 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy Map Configuration mode

**User Guidelines**

This command causes the specified policy to create a reference to the class definition. The command mode is changed to Policy-Class-Map Configuration when this command is executed successfully.
Example
The following example shows how to specify the DiffServ class name of “DELL.”

```
console(config)#class-map match-all DELL
console(config-classmap)#exit
console(config)#policy-map DELL1 in
console(config-policy-map)#class DELL
```

class-map
Use the class-map command in Global Configuration mode to define a new DiffServ class of type match-all. To delete an existing class, use the no form of this command.

Syntax
```
class-map [match-any | match-all] class-map-name

no class-map class-map-name
```

- class-map-name — a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.
- match-any—The class map will match if any of the specified criteria matches.
- match-all—The class map will match only if all of the specified criteria match.

Default Configuration
The class-map command has no defaults.

Command Mode
Global Configuration mode

User Guidelines
Enter the class-map command without the match-all/match-any parameter and an existing class-map-name to modify the named class map.
Enter the `class-map` command with the match-all/match-any parameter and a nonexistent class-map-name to create a new class map. The class-map-name must not be the same as any other class map or access group name.

Use the `no class-map` form of the command without a match-all/match-any parameter to delete an existing class map.

The match-all parameter indicates that all of the match criteria configured in the class map must be met for the packet to be processed by the class map.

The match-any parameter indicates that any of the match criteria configured in the class-map may be met for the packet to be processed by the class-map.

Only one access-group may be referenced in a match-all class map. Multiple access-groups of the same type may be referenced in a match-any class map.

**Command History**

Updated syntax in version 6.5 firmware.

**Example**

The following example creates a class-map named “DELL” which requires terms in the access-group DELL-ACCESS to be matched.

```
console(config)#class-map match-all DELL
console(config-classmap)#match access-group DELL-ACCESS
console(config-cmap)#exit
```

The following example configures multiple policy maps. Each policy map references a class map that references access groups. Assign the policy for inbound traffic to interfaces using the `service policy-in` command.

```
console(config)#ip access-list default
console(config-ip-acl)#deny   ip any any
console(config-ip-acl)#exit
console(config)#ip access-list voice-all
console(config-ip-acl)#permit udp 10.0.0.0 0.255.255.255 any range 16384 32768
console(config-ip-acl)#permit udp any 10.0.0.0 0.255.255.255 range 16384 32768
console(config-ip-acl)#permit udp 10.0.0.0 0.255.255.255 eq 17000 any
console(config-ip-acl)#deny   ip any any
console(config-ip-acl)#exit
console(config)#ip access-list voice-pass
console(config)#class-map match-any voice-all
```

```
console(config-classmap)#match access-group name voice-pass
console(config-classmap)#match access-group name voice-all
console(config)#exit
console(config)#class-map match-all port-default
console(config-classmap)#match access-group name default
console(config)#exit
console(config)#policy-map inbound in
console(config-policy-classmap)#class voice-all
console(config-policy-classmap)#mark ip dscp af41
console(config-policy-classmap)#exit
console(config-policy-classmap)#class port-default
console(config-policy-classmap)#mark ip dscp af21
console(config-policy-classmap)#exit
console(config-policy-classmap)#exit

**class-map rename**

Use the `class-map rename` command in Global Configuration mode to change the name of a DiffServ class.

**Syntax**

class-map rename classname newclassname

- **classname** — The name of an existing DiffServ class. (Range: 1–31 characters)
- **newclassname** — A case-sensitive alphanumeric string. (Range: 1–31 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example displays how to change the name of a DiffServ class from “DELL” to “DELL1.”

```
console(config)#class-map rename DELL DELL1
console(config)#
```

classofservice dot1p-mapping
Use the classofservice dot1p-mapping command in Global Configuration mode to map an IEEE 802.1p user priority to an internal traffic class. In Interface Configuration mode, the mapping is applied only to packets received on that interface. Use the no form of the command to remove mapping between an 802.1p priority and an internal traffic class.

Syntax
```
classofservice dot1p-mapping ppriority trafficclass
no classofservice dot1p-mapping
```

- **ppriority** — Specifies the user priority mapped to the specified traffic class for this switch. (Range: 0–7)
- **trafficclass** — Specifies the traffic class for this switch. (Range: 0–6)

Default Configuration
The default 802.1p mapping is as follows:

<table>
<thead>
<tr>
<th>User Priority</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</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>2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration or Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**
None

**Example**
The following example globally configures a mapping for user priority 1 and traffic class 2. If trust mode is enabled for 802.1p (classofservice trust dot1p), packets received on any interface marked with IEEE 802.1p priority 1 will be assigned to internal CoS queue 2.
```
console(config)#classofservice dot1p-mapping 1 2
```

**classofservice ip-dscp-mapping**
Use the `classofservice ip-dscp-mapping` command in Global Configuration mode to map an IP DSCP value to an internal traffic class. Use the `no` form of the command to return the classofservice mapping to the default, and remove a traffic class mapping for an IP DSCP value.

**Syntax**
```
classofservice ip-dscp-mapping ipdscp trafficclass
no classofservice ip-dscp-mapping
```
- **ipdscp**—Specifies the IP DSCP value which is to be mapped to the specified traffic class. (Range: 0–63 or an IP DSCP keyword – af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).
- **trafficclass**—Specifies the traffic class for this value mapping. (Range: 0–6).

**Default Configuration**
The default DSCP mapping is as follows:
<table>
<thead>
<tr>
<th>IP DSCP</th>
<th>Traffic Class (queue-id)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0(bc/cs0)</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8(cs1)</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>10(af11)</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>12(af12)</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>14(af13)</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>16(cs2)</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>18(af21)</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>20(af22)</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>22(af23)</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
</tr>
<tr>
<td>24(cs3)</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>26(af31)</td>
<td>1</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>Traffic Class (queue-id)</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>27</td>
<td>1</td>
</tr>
<tr>
<td>28(af32)</td>
<td>1</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
</tr>
<tr>
<td>30(af33)</td>
<td>1</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
</tr>
<tr>
<td>32(cs4)</td>
<td>2</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
</tr>
<tr>
<td>34(af41)</td>
<td>2</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
</tr>
<tr>
<td>36(af42)</td>
<td>2</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
</tr>
<tr>
<td>38(af43)</td>
<td>2</td>
</tr>
<tr>
<td>39</td>
<td>2</td>
</tr>
<tr>
<td>40(cs5)</td>
<td>2</td>
</tr>
<tr>
<td>41</td>
<td>2</td>
</tr>
<tr>
<td>42</td>
<td>2</td>
</tr>
<tr>
<td>43</td>
<td>2</td>
</tr>
<tr>
<td>44</td>
<td>2</td>
</tr>
<tr>
<td>45</td>
<td>2</td>
</tr>
<tr>
<td>46(ef)</td>
<td>2</td>
</tr>
<tr>
<td>47</td>
<td>2</td>
</tr>
<tr>
<td>48(cs6)</td>
<td>3</td>
</tr>
<tr>
<td>49</td>
<td>3</td>
</tr>
<tr>
<td>50</td>
<td>3</td>
</tr>
<tr>
<td>51</td>
<td>3</td>
</tr>
<tr>
<td>52</td>
<td>3</td>
</tr>
<tr>
<td>53</td>
<td>3</td>
</tr>
<tr>
<td>54</td>
<td>3</td>
</tr>
</tbody>
</table>
### Command Mode

Global Configuration mode

### User Guidelines

The switch may be configured to trust either DSCP or CoS values, but not both. Setting the trust mode does not affect ACL packet matching, e.g. it is still possible to use an ACL that matches on a received CoS value and assigns the packet to a queue even when DSCP is trusted.

### Example

The following example globally configures the mapping for IP DSCP 1 to traffic class 2. If trust mode is enabled for DSCP (classofservice trust ip-dscp), packets received on any interface marked with DSCP 1 will be assigned to internal CoS queue 2.

```
console(config)#classofservice ip-dscp-mapping 1 2
```

### classofservice trust

Use the classofservice trust command in either Global Configuration mode or Interface Configuration mode to set the class of service trust mode of an interface. To set the interface mode to trust 802.1p markings, use the no form of this command.
**Syntax**

classofservice trust {dot1p | untrusted | ip-dscp}

no classofservice trust

- **dot1p** — Specifies that the mode be set to trust IEEE 802.1p packet markings.
- **untrusted** — Sets the Class of Service Trust Mode to Untrusted.
- **ip-dscp** — Specifies that the mode be set to trust IP DSCP packet markings.

**Default Configuration**

By default, the switch trusts IEEE 802.1p markings.

**Command Mode**

Global Configuration mode or Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command has no user guidelines.

**Examples**

The following example sets the class of service trust mode of all interfaces to trust 802.1p packet markings.

```
console(config)#classofservice trust dot1p
```

The following example displays how to set the class of service trust mode of all interfaces to trust IP DSCP packet markings.

```
console(config)#classofservice trust ip-dscp
```

**conform-color**

Use the `conform-color` command in Policy-Class-Map Configuration mode to enable color-aware marking for a policy.

**NOTE:** This command is not available on the N1500 Series switches.
**Syntax**

conform-color {class-map-name} [exceed-color { class-map-name } ]

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode

**User Guidelines**

This command must be preceded by a police command. If the conform-color command is not entered, the police algorithm uses the color-blind version, meaning in the incoming color is ignored. The conform-color command can be used with any of the three police algorithms. In the simple algorithm, only the conform color class can be configured. The conform color class pre-colors packets as green prior to metering. Non-conforming packets are pre-colored red prior to metering. With the single-rate and two-rate police algorithm, the conform color class pre-colors packets as green and the exceed color class pre-colors packets as yellow. Non-conforming packets are pre-colored red. Per-colored packets are then metered and re-colored based upon the meter parameters.

Color conforming classes must be one of the following types:

- Primary COS
- Secondary COS
- DSCP
- IP Precedence

This includes both the input and color aware classes. The conform color class may not be the same as the input class, nor may the match criteria be of the same type. The input class map may have a match type of “any.”

The exceed color class may only be specified for the two-rate police algorithm.
Example
The following example uses a simple policer to color TCP packets that exceed an average rate of 1000 Kbps or a burst size of 16 Kbytes as red. Conforming packets (those in CoS queue 1) are pre-colored green prior to metering. After metering, non-conforming packets are colored red. Both green and red packets are transmitted, but may be subject to further color-based action on egress. The example configuration below also shows the configuration of WRED drop thresholds and probabilities for colored traffic.

```console
console(config)#class-map match-all class-ipv4
console(config-classmap)#match any
console(config-classmap)#exit
console(config)#class-map match-all class-cos1
console(config-classmap)#match cos 1
console(config-classmap)#exit
console(config)#policy-map color in
console(config-policy-map)#class class-ipv4
console(config-policy-classmap)#police-simple 1000 16 conform-action transmit violate-action transmit
console(config-policy-classmap)#conform-color class-cos1
console(config-policy-classmap)#exit
console(config-policy-map)#exit
```

cos-queue min-bandwidth

Use the `cos-queue min-bandwidth` command in either Global Configuration mode or Interface Configuration mode to specify the minimum transmission bandwidth for each interface queue. To restore the default for each queue’s minimum bandwidth value, use the `no` form of this command.

Syntax

cos-queue min-bandwidth bw-0 bw-1 … bw-n

no cos-queue min-bandwidth

-  `bw-0` — Specifies the minimum transmission bandwidth guarantee for an interface. You must specify as many bandwidth parameters as there are COS queues (bw-0 through bw-n). (Range: 0–100 in increments of 5)

Default Configuration

By default, all CoS queues are configured with a 0% minimum bandwidth guarantee.
**Command Mode**

Global Configuration mode or Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command changes the scheduling policy for packet transmission of the selected CoS queues. It does not change the packet buffering policy nor does it reserve packet buffers to a CoS queue.

The maximum number of queues supported per interface is seven. It is recommended that the operator avoid the use of queue 5-7 to avoid conflicts with inter- and intra-network control traffic.

In order to better accommodate bursty traffic, it is recommended that the sum of the configured min-bandwidths be much less than 100%. Configuring the minimum bandwidths such that they sum to 100% effectively locks the scheduler such that bandwidth sharing by lower priority queues cannot be accommodated under congestion conditions.

When ETS is operational on an N4000 series switch, this command overrides the ETS assignments and assigns minimum bandwidth constraints across traffic class groups. This allows the administrator to ensure that the frame scheduler does not completely starve lower priority groups when strict priority is enabled on a high numbered TCG. Specifically, assigning a minimum bandwidth to a lower numbered TCG, even when strict priority is enabled on a higher numbered TCG, will alter the normal scheduler behavior and cause the scheduler to process frames from the lower numbered TCG to conform to the min-bandwidth constraint.

**Example**

The following example displays how to specify the minimum transmission bandwidth guarantee for cos-queues 0 through 6 as follows:

Cos Queue 0—5% scheduler capacity
Cos Queue 1—5% scheduler capacity
Cos Queue 2—10% scheduler capacity
Cos Queue 3—10% scheduler capacity
Cos Queue 4-7—Shared scheduler capacity.

```
console(config)#cos-queue min-bandwidth 5 5 10 10 0 0 0
```
cos-queue random-detect

Use the cos-queue random-detect command in Global Configuration or Interface Configuration mode to enable WRED queue management policy on an interface CoS queue. Use the no form of the command to disable WRED policy for a CoS queue on an interface.

**NOTE:** On the N1500 Series switches, this command enables Simple RED since the hardware is not capable of Weighted RED.

**Syntax**

```plaintext
cos-queue {random-detect queue-id1 [queue-id2..queue-idn]}
no cos-queue {random-detect queue-id1 [queue-id2..queue-idn]}
```

- queue-id—An integer indicating the internal CoS queue-id which is to be enabled for WRED. Range 0-6. Up to 7 queues may be simultaneously specified.

**Default Configuration**

WRED queue management policy is disabled by default. Tail-drop queue management policy is enabled by default. The threshold for invoking tail-drop behavior when WRED is disabled is approximately 1/2 of the remaining free packet buffer in the switch.

**Command Mode**

Interface Configuration (physical or port-channel) mode, Interface Range mode, or Global Configuration mode

**User Guidelines**

When used on a port-channel, this command will override the settings on the individual interfaces that are part of the port channel. Removing an interface from the port channel restores the individual interface settings.

This command can be used in Interface Range mode.

Use the cos-queue min-bandwidth command to configure the minimum scheduler bandwidth percentage guarantee for the CoS queues.

Use the show interfaces random-detect command to display the WRED configuration, including ECN configuration.
Use the `policy-map` and `conform-color` commands to mark traffic with a color other than default green color.

The drop probability scale supports values in the range 0-10% and the discrete values 25%, 50%, 75%, and 100%. Other values are truncated to the next lower value by the hardware.

### N1500 Series Switches

N1500 Series switches support a simple RED capability. The N1500 Series switch does not support configuration of the maximum threshold nor can the threshold or drop probability be configured for non-TCP traffic. Only the minimum threshold (min-thresh) and drop probability (drop-prob-scale) may be configured for the TCP colors green/yellow/red. The maximum threshold may not be configured nor can the threshold or drop probability be configured for non-TCP traffic. ECN capability is supported.

Simple RED may be enabled/disabled for any CoS queue on the Dell EMC Networking N1500 Series switches, however, the drop probability must be one of the values given below. The percentage before the dash indicates the actual drop probability. The number after the dash indicates the value entered in the drop-prob-scale parameter.

- 0.097% - 1
- 0.195% - 2
- 0.391% - 4
- 0.781% - 8
- 1.563% - 16
- 3.125% - 31
- 6.250% - 63
- 100% - 100

### Examples

**Example 1**

This example enables WRED on internal CoS 0 queue for unmarked packets and set the green, yellow, and red colored traffic to utilize WRED starting at 3% of port congestion with a drop probability of 1%, 2% and 3%, respectively. In this configuration, non-TCP traffic uses tail-drop queue discipline with a
drop threshold at 100% of the statically calculated port queue length vs. the
dynamically calculated value used by the normal tail-drop mechanism
(approx. 1/2 remaining free packet buffer memory).

```console
console(config)# cos-queue random-detect 0
console(config)# random-detect queue-parms 0 min-thresh 3 3 3 100 max-thresh
10 10 10 100 drop-prob-scale 1 2 3 0
```

**Example 2**

This example configures simple RED on an N1500 series switch. CoS queue 1
is globally configured for simple RED with a congestion threshold of 50% and
a drop probability of 0.781% for green colored traffic.

```console
console(config)# random-detect queue-parms 1 min-thresh 50 0 0 drop-prob-
scale 8 0 0
console(config)#cos-queue random-detect 1
```

**cos-queue strict**

Use the `cos-queue strict` command in either Global Configuration mode or
Interface Configuration mode to activate the strict priority scheduler mode
for the specified queue. To restore the default weighted scheduler mode for
each specified queue, use the `no` form of this command.

**Syntax**

```plaintext
cos-queue strict {queue-id-1} [{queue-id-2} ... {queue-id-n}]
no cos-queue strict {queue-id-1} [{queue-id-2} ... {queue-id-n}]
```

- **queue-id-1** — Specifies the queue ID for which you are activating the
  strict priority scheduler. You can specify a queue ID for as many queues as
  you have (queue-id 1 through queue-id-n). (Range: 0–6)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode or Interface Configuration (gigabitethernet,
port-channel, tengigabitethernet, fortygigabitethernet) mode
User Guidelines

Strict priority (SP) queues are scheduled in priority order ahead of WRR queues. Strict priority queues are allocated unlimited bandwidth by default. Configuring the min-bandwidth on a CoS queue also configured for strict priority wastes the scheduler slots. Use the `cos-queue min-bandwidth` command on lower priority SP and WRR queues to ensure fairness to lower priority queues by reserving a specific amount of scheduler bandwidth. Use the `show interfaces cos-queue` command to display the class of service settings.

Strict priority scheduling is most useful when it is desirable that low-bit-rate time-sensitive traffic be queued ahead of other traffic. The administrator must be careful to limit the bandwidth assigned to the strict priority queue to avoid potential denial of service attacks. See the “Enterprise Voice VLAN Configuration With QoS” section in the Users Configuration Guide for a rate limiting example. If using the min-bandwidth command to reserve bandwidth on other queues, ensure that the total of the minimum bandwidths is less than 100% to allow the scheduler to handle bursts of traffic.

Example

The following example displays how to activate the strict priority scheduler mode for two queues.

```
cos-queue strict 1 2
```

The following example displays how to activate the strict priority scheduler mode for three queues (1, 2, and 4) and reserves a minimal amount of bandwidth on the other four internal CoS queues (0, 3, 5 and 6).

```
cos-queue strict 1 2 4
```
```
cos-queue min-bandwidth 5 0 0 10 0 10 10
```

diffserv

Use the `diffserv` command in Global Configuration mode to set the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not operational. When enabled, DiffServ services are operational on queues configured for WRED. To set the DiffServ operational mode to inactive, use the `no` form of this command.
NOTE: On the N1500 Series switches, enable Simple RED since the hardware is not capable of Weighted RED.

Syntax

diffserv
no diffserv

Default Configuration
This command default is enabled.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example displays how to set the DiffServ operational mode to active.

```
console(Config)#diffserv
```

**drop**

Use the `drop` command in Policy-Class-Map Configuration mode to specify that all packets for the associated traffic stream are to be dropped at ingress.

NOTE: This command is not available on the N1500 Series switches.

Syntax

drop

Default Configuration
This command has no default configuration.

Command Mode
Policy-Class-Map Configuration mode
**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays how to specify that matching packets are to be dropped at ingress.

```
console(config-policy-classmap)#drop
```

**mark cos**
Use the `mark cos` command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified class of service value in the user priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

- **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**
```
mark cos cos-value
```

- cos-value — Specifies the CoS value as an integer. (Range: 0–7)

**Default Configuration**
There is no default cos-value for this command. Packets are not remarked by default.

**Command Mode**
Policy-Class-Map Configuration mode

**User Guidelines**
Received frames are assigned to an internal CoS queue on ingress depending on configuration such as whether the ingress port is trusted for CoS, DSCP or IP precedence value and it's mapping onto an internal CoS queue.

Frames may be remarked using either an **in** or an **out** policy map. Changing the CoS value in the VLAN tag of a frame does not alter the internal CoS assigned to the packet; it only rewrites the CoS value in the Ethernet frame header.
Example
The following example displays how to mark all packets with a CoS value.

```
console(config-policy-classmap)#mark cos 7
```

mark ip-dscp

Use the mark ip-dscp command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP DSCP value.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

Syntax
```
mark ip-dscp dscpval
```
- **dscpval** — Specifies a DSCP value (10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38, 0, 8, 16, 24, 32, 40, 48, 56, 46) or a DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

Default Configuration
This command has no default configuration.

Command Mode
Policy-Class-Map Configuration mode

User Guidelines
Received frames are assigned to a CoS queue on ingress depending on configuration items such as whether the ingress port is trusted for CoS, DSCP or IP precedence value and it's mapping onto an internal CoS queue.

IP packets may be remarked using either an `in` or an `out` policy map.
Changing the IP DSCP value in the ToS value of an IP packet does not alter the internal CoS assigned to the packet; it only rewrites the ToS value in the IP packet header.
Example
The following example displays how to mark all packets with an IP DSCP value of “cs4.”

console(config-policy-classmap)#mark ip-dscp cs4

mark ip-precedence

Use the `mark ip-precedence` command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP precedence value.

**NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

`mark ip-precedence prec-value`

- `prec-value` — Specifies the IP precedence value as an integer. (Range: 0–7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode

**User Guidelines.**

Received frames are assigned to a CoS queue on ingress depending on configuration such as whether the ingress port is trusted for CoS, DSCP or IP precedence value and it's mapping onto an internal CoS queue.

IP packets may be remarked using either an `in` or an `out` policy map. Changing the IP precedence value in the ToS value field of an IP packet does not alter the internal CoS assigned to the packet; it only rewrites the ToS value in the IP packet header.

**Example**

The following example displays

console(config)#policy-map p1 in
console(config-policy-map)#class c1
match access-group

Use the **match access-group** command to add ACL match criteria to a class map. Use the **no** form of the command to remove the ACL match criteria.

**Syntax**

```
match access-group name name
no match access-group name name
```

- name—The name of an access-list. Only MAC, IPv4, and IPv6 access-lists are allowed.

**Default Configuration**

No access-lists are configured for a class-map.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

ACLs are used to classify traffic and class/policy maps are used to define the QoS treatment of the traffic class. The ACL is used for classification only, and the result of classification is match or not match. Access-groups identified in a class-map are applied in order of appearance in the class-map declaration (regardless of ACL number). ACLs in an access-group are applied in order of ACL number.

Access-groups may only be specified in ingress class maps. The clauses in an access-list referenced in a class-map are used solely to match (or not match) traffic. Action (set/drop/mirror/rate-limit) clauses in ACLs referenced by a policy are ignored for the purposes of policy application.

The permit and deny clauses have a different meaning than that used in a standard ACL.
If a packet matches a permit ACL clause specified in a class-map, the packet matches, no further matching is performed, and the class-map clause is matched.

If a packet matches a deny ACL class specified in a class-map, the packet does not match, no further matching is performed, and the class-map clause is not matched.

No counters are instantiated for ACLs referenced in a class map.

**Command History**

Command introduced in version 6.5 firmware.

**Example**

The following example configures an access list arp-list with a policy that implements a simple policer for ARP packets coming from any of the hosts listed in the access list. The policer operates on the aggregate bandwidth of the matched packet streams.

```
console(config)#mac access-list extended arp-list
console(config-mac-access-list)#permit 00:01:02:03:04:05 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:07 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:08 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:01 0000.0000.0000 any 0x0806
console(config-mac-access-list)#exit
console(config)#class-map match-any class-arp
console(config-classmap)#match protocol none
console(config-classmap)#match access-group arp-list
console(config-classmap)#exit
console(config)#policy-map arp-limiter in
console(config-policy-map)#class class-arp
console(config-policy-classmap)#police-simple 1000 16 conform-action transmit violate-action drop
console(config-policy-classmap)#exit
console(config-policy-map)#exit
```

The above policy must be configured on one or more interfaces to be enabled.
**match class-map**

Use the `match class-map` command to add to the specified class definition the set of match conditions defined for another class. Use the `no` form of this command to remove from the specified class definition the set of match conditions defined for another class.

[NOTE: This command is not available on the N1500 Series switches.]

**Syntax**

```plaintext
match class-map refclassname

no match class-map refclassname
```

- `refclassname` — The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

- The parameters `refclassname` and `class-map-name` can not be the same.
- Only one other class may be referenced by a class.
- Class maps may be chained, for example, a class-map may reference another class map, which references a third class map, et seq.
- Any attempts to delete the `refclassname` class while the class is still referenced by any class-map-name fails.
- The combined match criteria of `class-map-name` and `refclassname` must be an allowed combination based on the class type.
- Any subsequent changes to the `refclassname` class match criteria must maintain this validity, or the change attempt fails.
• The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

**Example**
The following example adds match conditions defined for the Dell class to the class currently being configured.

```console
console(config-classmap)#match class-map Dell
```

The following example deletes the match conditions defined for the Dell class from the class currently being configured.

```console
console(config-classmap)#no match class-map Dell
```

**match cos**

Use the `match cos` command in Class-Map Configuration mode to add a match condition for the class of service value (the only tag in a single-tagged packet or the first or outer 802.1Q tag of a double-VLAN tagged packet).

![NOTE](image)

*NOTE:* This command is not available on the N1500 Series switches.

**Syntax**

```
match cos
```

- `cos-value` — Specifies the CoS value as an integer (Range: 0–7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example displays adding a match condition to the specified class.

console(config-classmap)#match cos 1

**match destination-address mac**

Use the **match destination-address mac** command in Class-Map Configuration mode to add a match condition based on the destination MAC address of a packet.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

```
match destination-address mac macaddr macmask
```

- **macaddr** — Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- **macmask** — Specifies a valid layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This address bit mask does not need to be contiguous.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures a match condition for the specified MAC address and bit mask.

```
```
match any

Use the **match any** command in Class-Map Configuration mode to allow matching on any of the specified match conditions. Use the **no** form of the command to remove the ACL match criteria and revert to match-all behavior.

**Syntax**

```
match any
no match any
```

**Default Configuration**

The default matching for a class map is to match on all specified match conditions.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

The clauses in an access-list referenced in a class-map are used solely to match (or not match) traffic. Access-groups identified in a class-map are matched in order of appearance in the class-map declaration (regardless of ACL number). ACLs in an access-group are matched in order of ACL number.

Unlike the match all condition, when a class-map contains the match any condition, the first match for a permit or deny immediately exits the matching activity for the class-map. Conceptually, the permit/deny clauses in the access group are applied sequentially.

In the match all scenario, the permit/deny clauses in the access group are applied in parallel, and all conditions must match for the matching activity to exit. For this reason, it is not advised to mix permit and deny clauses within an access-group used in a match all class map.

**Command History**

Command introduced in version 6.5 firmware.
Example

The following example configures a MAC access list arp-list with a policy that implements a simple policer for ARP packets coming from any of the hosts listed in the access list. Apply the policy to an interface using the service-policy in command in Interface Configuration mode.

```
console(config)#mac access-list extended arp-list
console(config-mac-access-list)#permit 00:01:02:03:04:05 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:07 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:08 0000.0000.0000 any 0x0806
console(config-mac-access-list)#permit 00:03:04:05:06:01 0000.0000.0000 any 0x0806
console(config-mac-access-list)#exit
console(config)#class-map match-any class-arp
console(config-classmap)#match protocol none
console(config-classmap)#match access-group name arp-list
console(config-classmap)#exit
console(config)#policy-map arp-limiter in
console(config-policy-map)#class class-arp
console(config-policy-classmap)#police-simple 1000 16 conform-action transmit violate-action drop
console(config-policy-classmap)#exit
console(config-policy-map)#exit
```

match dstip

Use the match dstip command in Class-Map Configuration mode to add a match condition based on the destination IP address of a packet.

⚠️ NOTE: This command is not available on the N1500 Series switches.

Syntax

```
match dstip ipaddr ipmask
```

- `ipaddr` — Specifies a valid IP address.
- `ipmask` — Specifies a valid IP address bit mask. Note that even though this parameter is similar to a standard subnet mask, it does not need to be contiguous.
**Default Configuration**
This command has no default configuration.

**Command Mode**
Class-Map Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays adding a match condition using the specified IP address and bit mask.

```
console(config-classmap)#match dstip 10.240.1.1 255.255.255.1
```

**match dstip6**
The `match dstip6` command adds a match condition based on the destination IPv6 address of a packet.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**
```
match dstip6 destination-ipv6-prefix/prefix-length
```
- destination-ipv6-prefix—IPv6 prefix in IPv6 global address format.
- prefix-length—IPv6 prefix length value.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Ipv6-Class-Map Configuration mode.

**User Guidelines**
There are no user guidelines for this command.
Example
console(config-classmap)#match dstip6 2001:DB8::0/32

match dstl4port

Use the **match dstl4port** command in Class-Map Configuration mode to add a match condition based on the destination layer 4 port of a packet using a single keyword or a numeric notation.

NOTE: This command is not available on the N1500 Series switches.

**Syntax**

match dstl4port {portkey | port-number}

- **portkey** — Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
- **port-number** — Specifies a layer 4 port number (Range: 0–65535).

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays adding a match condition based on the destination layer 4 port of a packet using the “echo” port name keyword.

console(config-classmap)#match dstl4port echo

match ethertype

Use the **match ethertype** command in Class-Map Configuration mode to add a match condition based on the value of the ethertype.
NOTE: This command is not available on the N1500 Series switches.

Syntax

match ethertype {keyword | 0x0600-0xffff}

- keyword — Specifies either a valid keyword or a valid hexadecimal number. The supported keywords are appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsunicast, mplsunicast, netbios, novell, pppoe, rarp. (Range: 0x0600–0xFFFF)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a match condition based on ethertype.

```
console(config-classmap)#match ethertype arp
```

**match ip6flowlbl**

The **match ip6flowlbl** command adds to the specified class definition a match condition based on the IPv6 flow label of a packet.

NOTE: This command is not available on the N1500 Series switches.

Syntax

match ip6flowlbl label

- label - The value to match in the Flow Label field of the IPv6 header (Range 0-1048575).
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Ipv6-Class-Map Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example adds a rule to match packets whose IPv6 Flow Label equals 32312.

```
console(config-classmap)#match ip6flowlbl 32312
```

**match ip dscp**
Use the `match ip dscp` command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet.

**NOTE:** This command is not available on the N1500 Series switches.

**Syntax**
```
match ip dscp dscpval
```
• `dscpval` — Specifies an integer value or a keyword value for the DSCP field. (Integer Range: 0–63) (Keyword Values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Class-Map Configuration mode
User Guidelines

This DSCP field is defined as the high-order six bits of the Service type octet in the IP header. The low-order two bits are not checked.

The `ip dscp`, `ip precedence`, and `ip tos` match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all DSCP values, use the `match ip tos` `tosbits` `tosmask` command with `tosbits` set to “0” (zero) and `tosmask` set to hex “03.”

Example

The following example displays how to add a match condition based on the DSCP field.

```
console(config-classmap)# match ip dscp 3
```

match ip precedence

Use the `match ip precedence` command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP precedence field.

NOTE: This command is not available on the N1500 Series switches.

Syntax

```
match ip precedence precedence
```

- precedence — Specifies the precedence field in a packet. This field is the high-order three bits of the Service Type octet in the IP header. (Integer Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode
User Guidelines

The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all precedence values, use the match ip tos tosbits tosmask command with tosbits set to “0” (zero) and tosmask set to hex “1F.”

Example

The following example displays adding a match condition based on the value of the IP precedence field.

```
console(config-classmap)#match ip precedence 1
```

**match ip tos**

Use the match ip tos command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP TOS field in a packet. This field is defined as all eight bits of the Service Type octet in the IP header.

⚠️ NOTE: This command is not available on the N1500 Series switches.

**Syntax**

```
machine ip tos [tosbits tosmask]
```

- **tosbits** — Specifies a two-digit hexadecimal number. (Range: 00–ff)
- **tosmask** — Specifies the bit positions in the tosbits parameter that are used for comparison against the IP TOS field in a packet. This value of this parameter is expressed as a two-digit hexadecimal number. (Range: 00–ff)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode
User Guidelines

The `ip dscp`, `ip precedence`, and `ip tos` match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

This specification is the free form version of the IP DSCP/Precedence/TOS match specification in that you have complete control of specifying which bits of the IP Service Type field are checked.

Example

The following example displays adding a match condition based on the value of the IP TOS field in a packet.

```
console(config-classmap)#match ip tos AA EF
```

match protocol

Use the `match protocol` command in Class-Map Configuration mode to match packets using the EtherType field in the Ethernet frame header. For certain protocols, an additional match condition for the IP protocol number is performed.

```
NOTE: This command is not available on the N1500 Series switches.
```

Syntax

```
match protocol {icmp|igmp|ip|ipv6|tcp|udp|gre|icmpv6
     |<identifier>|none }
```

Ethertype only matches:

- `ip`—Match IPv4 protocol packets (Ethertype 0x0800)
- `ipv6`—Match IPv6 protocol packets (Ethertype 0x86dd)
- `<identifier>`—A numerical value (0x0-255) identifying an IPv4 or IPv6 protocol.

Ethertype and Protocol matches:

- `none`—Remove the default or configured Ethertype/Protocol match criteria. Configure a MAC access-group match.
- `icmp`—Match ICMP protocol packets (Ethertype 0x0800 and IPv4 protocol 1).
- igmp—Match IGMP protocol packets (Ethertype 0x0800 and IPv4 protocol 2).
- tcp—Match TCP packets (Ethertype 0x0800 and IPv4 protocol 6 or Ethertype 0x86dd and IPv6 Next Header 6)
- udp—Match UDP packets (Ethertype 0x0800 and IPv4 protocol 17 or Ethertype 0x86dd and IPv6 Next Header 17)
- gre—Match GRE protocol packets (Ethertype 0x0800 and IPv4 protocol 47 or Ethertype 0x86dd and IPv6 Next Header 47)
- icmpv6—Match IPv6 ICMP packets (Ethertype 0x86dd and IPv6 Next Header 58)

**Default Configuration**

The default is match protocol ip (Ethertype 0x0800).

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

Use the `match protocol none` command to remove any match condition for Ethertype or Protocol number. Only one Ethertype match protocol statement can appear in a class-map. Entering a match protocol statement overrides any prior protocol match.

Prior to entering a `match access-group` command other than type IPv4 in class-map configuration mode, it is necessary to enter the corresponding `match protocol` command. For example, to match an IPv6 access-group, issue the `match protocol ipv6` command first. Use `match protocol none` to match a MAC access-group. Only a single `match protocol` command may be issued.

If an ACL is referenced in the class-map, it must be of the same type as the configured Ethertype.

If the `match ethertype` command is configured, `match protocol` may not be configured, and vice versa.

**Command History**

Command introduced in version 6.5 firmware
Example
The following example displays adding a match condition based on the “ip” protocol name keyword.

```
console(config-classmap)#match protocol ip
```

**match source-address mac**

Use the `match source-address mac` command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source MAC address of the packet.

⚠️ NOTE: This command is not available on the N1500 Series switches.

**Syntax**

```
match source-address mac address macmask
```

- `macaddr` — Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- `macmask` — Specifies a layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This bit mask does not need to be contiguous.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example adds to the specified class definition a match condition based on the source MAC address of the packet.

```
console(config-classmap)# match source-address mac 10:10:10:10:10:10
11:11:11:11:11:11
```
**match srcip**

Use the `match srcip` command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source IP address of a packet.

> NOTE: This command is not available on the N1500 Series switches.

**Syntax**

```
match srcip ipaddr ipmask
```

- **ipaddr** — Specifies a valid IP address.
- **ipmask** — Specifies a valid IP address bit mask. Note that although this IP address bit mask is similar to a subnet mask, it does not need to be contiguous.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Class-Map Configuration mode

**User Guidelines**

Only one srcip matching criteria can be specified. To remove the matching criteria, delete the class map.

**Example**

The following example displays adding a match condition for the specified IP address and address bit mask.

```
console(config-classmap)#match srcip 10.240.1.1 10.240.0.0
```

**match srcip6**

The `match srcip6` command adds to the specified class definition a match condition based on the source IPv6 address of a packet.

> NOTE: This command is not available on the N1500 Series switches.
Syntax
match srcip6 source-ipv6-prefix/prefix-length
  • source-ipv6-prefix — IPv6 prefix in IPv6 global address format.
  • prefix-length — IPv6 prefix length value.

Default Configuration
There is no default configuration for this command.

Command Mode
Ipv6-Class-Map Configuration mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-classmap)#match srcip6 2001:DB8::0/32

match srccl4port
Use the match srccl4port command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or a numeric notation.

NOTE: This command is not available on the N1500 Series switches.

Syntax
match srccl4port {portkey | port-number}
  • portkey — Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
  • port-number — Specifies a layer 4 port number (Range: 0–65535).

Default Configuration
This command has no default configuration.
Command Mode
Class-Map Configuration mode

User Guidelines
Only one srcl4port matching criteria can be specified. To remove the matching criteria, delete the class map.

Example
The following example displays how to add a match condition using the “snmp” port name keyword.

console(config-classmap)#match srcl4port snmp

match vlan

Use the match vlan command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field. This field is the only tag in a single tagged packet or the first or outer tag of a double VLAN packet.

NOTE: This command is not available on the N1500 Series switches.

Syntax
match vlan vlan-id

- vlan-id — Specifies a VLAN ID as an integer. (Range: 1-4093)

Default Configuration
This command has no default configuration.

Command Mode
Class-Map Configuration mode

User Guidelines
Only a single VLAN can be specified for each class map. To remove the matching criteria, delete the class map.
Example
The following example displays adding a match condition for the VLAN ID “2.”

```
console(config-classmap)#match vlan 2
```

**mirror**

Use the `mirror` command in Policy-Class-Map Configuration mode to mirror all the data that matches the class defined to the destination port specified.

- **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

```
mirror interface
```

- **interface** — Specifies the Ethernet port to which data needs to be copied.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode

**User Guidelines**

The port identified in this command is identical to the destination port of the `monitor` command.

**Example**

The following example displays how to copy all the data to port Gi1/0/5.

```
console(config-policy-classmap)#mirror gi1/0/5
```

**police-simple**

Use the `police-simple` command in Policy-Class-Map Configuration mode to applying a policing meter for the specified class.

- **NOTE:** This command is not available on the N1500 Series switches.
**Syntax**

```

- **datarate** — Data rate in kilobits per second (Kbps). (Range: 1–4294967295)
- **burstsize** — Burst size in Kbytes (Range: 1–128)
- **conform action** — Configures the action taken for packets that do not exceed the data rate or the burst size:
  - **drop**: Drop the packet.
  - **sec-prec-transmit ip-prec**: Remark the IP precedence in the packet to ip-prec and transmit. (Range 0-7)
  - **set-dscp-transmit dscp-val**: Remark the DSCP in the packet to dscp-val and transmit. (Range 0-63)
  - **set-cos-transmit 802.1p-priority**: Remark the 802.1p priority in the packet to 802.1p-priority and transmit. (Range 0-7)
  - **transmit**: Transmit the packet unmodified.

The same actions are available for packets that violate the policing rule.

- **violate-action** — Configures the action taken for packets that exceed the data rate or burst size.
  - **cos** — Class of Service value. (Range: 0–7)
  - **dscpval** — DSCP value. (Range: 0–63 or a keyword from this list: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode
User Guidelines

The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. Conforming packets are colored green and non-conforming packets are colored red for use by the WRED mechanism. Only one style of police command (simple, single-rate or two-rate) is allowed for a given class instance in a particular policy. The conform-color command can be used to pre-color packets prior to policing. Packets pre-colored red are not re-colored by the policer.

Example

The following example configures a single rate ingress meter with packets received at a rate below 1000 Kbps and 4096 byte burst size are transmitted and packets above that rate are dropped. The transmitted packets are colored green should the operator desire to configure a WRED drop policy.

```
console(config-policy-classmap)#police-simple 1000 64 conform-action transmit violate-action drop
```

police-single-rate

Use the police-single-rate command to implement a single-rate Three Color Market (srTCM) per RFC 2697.

NOTE: This command is not available on the N1500 Series switches.

Syntax

```
police-single-rate datarate burstsize excess-burstsize conform-action action exceed-action action violate-action action
```

- datarate—Data rate in kilobits per second (Kbps). (Range 1-4294967295)
- burstsize—Burst size in kilobits per seconds (Kbps). (Range 1-128)
- excess-burstsize—Excess burst size in kilobits per seconds (Kbps). (Range 1-128)
- action—The action to take according to the color. Select one:
  - drop: Drop the packet.
  - set-prec-transmit ip-prec: Remark the IP precedence in the packet to ip-prec and transmit. (Range 0-7)
Layer 2 Switching Commands

- **set-dscp-transmit** dscp-val: Remark the DSCP in the packet to dscp-val and transmit. (Range 0-63)
- **set-cos-transmit** 802.1p-priority: Remark the 802.1p priority in the packet to 802.1p-priority and transmit. (Range 0-7)
- **transmit**: Transmit the packet unmodified.

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Policy-Class-Map Configuration mode

**User Guidelines**

An srTCM meters a traffic stream and colors packets according to three parameters: Committed Information Rate (CIR), Committed Burst Size (CBS), and Peak Burst Size (PBS). A packet is colored red if it exceeds the CBS and the PBS, yellow if it exceeds the CBS, but not the PBS, and green if it exceeds neither. An srTCM is useful in situations where only the length of the burst, but not the peak rate, determines the service assignment.

The CIR is measured in Kbps, the CBS in Kbytes, and the PBS in Kbytes. It is recommended that the CBS and PBS be configured to be larger than the largest expected IP packet. A class command in policy-map mode must be issued for an existing class-map before entering this command.

**Example**

console(config-policy-classmap)#police-single-rate 100000000 32 64 conform-action set-cos-transmit 7 exceed-action set-prec-transmit 7 violate-action drop

**police-two-rate**

Use the **police-two-rate** command to implement a two-rate Three Color Market (trTCM) per RFC 2698.

![NOTE: This command is not available on the N1500 Series switches.](image)
Syntax

```
police-two-rate datarate burstsize peak-data-rate excess-burstsize conform-action action exceed-action action violate-action action
```

- **datarate** — Data rate in kilobits per second (Kbps). (Range: 1–4294967295)
- **burstsize** — Burst size in Kbytes (Range: 1–128)
- **peak-data-rate** — Peak data rate in kilobits per second (Kbps). (Range 1-4294967295)
- **excess-burstsize** — Excess burst size in kilobits per seconds (Kbps). (Range 1-128)
- **action** — The action to take according to the color. Select one of:
  - **drop** — Drop the packet.
  - **set-prec-transmit** ip-prec — Remark the IP precedence in the packet to ip-prec and transmit. (Range 0-7)
  - **set-dscp-transmit** dscp-val — Remark the DSCP in the packet to dscp-val and transmit. (Range 0-63)
  - **set-cos-transmit** 802.1p-priority — Remark the 802.1p priority in the packet to 802.1p-priority and transmit. (Range 0-7)
  - **transmit** — Transmit the packet unmodified.

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

A trTCM meters a traffic stream and colors packets according to four parameters:
- Committed Information Rate (CIR)
- Committed Burst Size (CBS)
- Peak Information Rate (PIR)
Peak Burst Size (PBS)
A packet is colored red if it exceeds the PIR, yellow if it exceeds the CIR, but not the PIR, and green if it does not exceed either. A trTCM is useful when a peak rate needs to be enforced separately from a committed rate.

The CIR and PIR are measured in Kbps (not pps as indicated in the RFC), the CBS in Kbytes, and the PBS in Kbytes. It is recommended that the CBS and PBS be configured to be larger than the largest expected IP packet. A class command in policy-map mode must be issued for an existing class-map before entering this command.

Example
console(config-policy-classmap)#police-two-rate 100000000 64 1000000000 32 conform-action set-cos-transmit 7 exceed-action set-prec-transmit 7 violate-action drop

policy-map
Use the policy-map command in Global Configuration mode to establish a new DiffServ policy or to enter policy map configuration mode. To remove the policy, use the no form of this command.

NOTE: This command is not available on the N1500 Series switches.

Syntax
policy-map policymame [in|out]
no policy-map policymame

- policymame—Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string of characters. (Range: 1–31 alphanumeric characters.)
- in—The policy is applied on ingress. Must be specified to create new DiffServ policies. An existing policy can be selected without specifying “in” or “out”.
- out—The policy is applied on egress. Either “in” or “out” must be specified to create a new DiffServ policy. An existing policy may be selected without the “in” or “out” parameter.
**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

The CLI mode is changed to Policy-Class-Map Configuration when this command is successfully executed.

The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

**Example**

The following example shows how to establish a new ingress DiffServ policy named “DELL.”

```
console(config)#policy-map DELL in
console(config-policy-classmap)#
```

**random-detect queue-parms**

Use the random-detect queue-parms command to configure the WRED green, yellow, and red TCP and non-TCP packet minimum and maximum drop thresholds and corresponding drop probabilities on an interface or globally.

**NOTE:** On the N1500 Series switches, enable Simple RED since the hardware is not capable of Weighted Red.

**Syntax**

```
random-detect queue-parms queue-id [queue-id] ... min-thresh minthresh-green minthresh-yellow minthresh-red minthresh-nontcp max-thresh max-thresh-green max-thresh-yellow max-thresh-red maxthresh-nontcp drop-prob-scale drop-scale-green drop-scale-yellow drop-scale-red drop-scale-nontcp [ecn ]
no random-detect queue-parms queue-id [queue-id] ...
```
• queue-id—The internal class of service queue (range 0-6). The queue-id is not the same as the CoS value received in incoming packets. Use the `show classofservice dot1p-mapping` command to display the CoS value to internal CoS queue mapping.

• min-thresh—The minimum threshold at which to begin dropping, based on the configured maximum drop probability for each color and for non-TCP packets. Range 0 to 250. At or below the minimum threshold, no packets are dropped. The range between the minimum and maximum thresholds is divided equally into eight increasing levels of drop probability.

• max-thresh—The maximum threshold to end dropping at the configured maximum drop probability for each color and for non-TCP packets. Range 0 to 250. Above the maximum threshold, 100% of matching packets are dropped.

• drop-prob-scale—The maximum drop probability. Range 0-100. This is the drop probability for a packet when the maximum threshold is reached. Above the maximum threshold, 100% of matching packets are dropped.

• ecn—Enables ECN marking for the selected CoS queues. Packets marked as ECN capable are not dropped when selected for discard by WRED.

**Default Configuration**

The table below shows the default green, yellow, and red TCP and non-TCP minimum maximum drop thresholds and the green, yellow and red TCP and non-TCP drop probabilities. The thresholds for each color and CoS queue are configured independently and may overlap. By default, WRED is not enabled for any CoS queue and ECN is not enabled for any CoS queue.

<table>
<thead>
<tr>
<th>Queue ID</th>
<th>WRED Minimum Threshold</th>
<th>WRED Maximum Threshold</th>
<th>WRED Drop Probability Scale</th>
<th>ECN Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>40/30/20/100</td>
<td>100/90/80/100</td>
<td>10/10/10/10</td>
<td>No</td>
</tr>
<tr>
<td>1</td>
<td>40/30/20/100</td>
<td>100/90/80/100</td>
<td>10/10/10/10</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>40/30/20/100</td>
<td>100/90/80/100</td>
<td>10/10/10/10</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>40/30/20/100</td>
<td>100/90/80/100</td>
<td>10/10/10/10</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>40/30/20/100</td>
<td>100/90/80/100</td>
<td>10/10/10/10</td>
<td>No</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration mode, Interface Configuration mode (physical and port-channel), Interface Range mode

User Guidelines

Interface configuration overrides the global configuration.

WRED Processing

WRED is intended to provide feedback to protocols (e.g. TCP) that depend on packet loss to adjust their transmission rate. WRED drop behavior only occurs when an interface is congested within the ranges specified. If congestion exceeds the upper limit, queued packets will be dropped at the rate of traffic ingressing the system, e.g. 100%. If the congestion is less than the lower limit, no packets will be dropped.

Traffic ingressing the switch can be assigned to one of four drop precedences based on a set of matching criteria. There are 3 drop precedences for TCP traffic (green, yellow, and red) and one drop precedence for non-TCP traffic (all colors). Users may configure the congestion thresholds at which packets experiencing congestion are dropped randomly for each drop precedence and may also configure the probability of a packet being dropped.

Packets are dropped at 100% when the egress queue size exceeds the maximum value and at 0% when the queue size is below the minimum value.

Configuring a queue with a drop probability of 0% effectively applies tail-drop behavior when the queue length exceeds the maximum threshold.

If the max-thresh parameter is less than the corresponding min-thresh parameter, it is adjusted to be the min-thresh plus one.

For a given network, the minimum and maximum WRED thresholds should be calculated to give a reasonable amount of buffering to TCP flows given the switch buffer capacity. WRED thresholds are applied individually to each

<table>
<thead>
<tr>
<th>Queue ID</th>
<th>WRED Minimum Threshold</th>
<th>WRED Maximum Threshold</th>
<th>WRED Drop Probability Scale</th>
<th>ECN Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>40/30/20/100</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>40/30/20/100</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>No</td>
</tr>
</tbody>
</table>
physical interface. For the Dell EMC Networking N2000/N3000 Series switches, a threshold of 100% corresponds to a buffer occupancy of 295428 bytes queued for transmission on an interface. For the N4000 Series switch, a threshold of 100% corresponds to a buffer occupancy of 666757 bytes queued for transmission on an interface.

Use the `classofservice dot1p-mapping` command or the `classofservice ip-dscp-mapping` command in conjunction with the `classofservice trust` command to assign packets to a CoS queue based upon values contained within the packet.

**WRED Drop Probabilities:**

Between the minimum and maximum thresholds, the drop probability is divided into eight discrete levels of increasing probability of packet drop. The levels are as follows:

0 - 6.25% of maximum drop probability
1 - 18.75% of maximum drop probability
2 - 30.25% of maximum drop probability
3 - 43.75% of maximum drop probability
4 - 56.25% of maximum drop probability
5 - 68.75% of maximum drop probability
6 - 81.25% of maximum drop probability
7 - 92.75% of maximum drop probability

As an example, with a drop probability of 50%, a minimum threshold of 10% and a maximum threshold of 90%, the drop probability from 10% to 20% congestion is 3.125%, from 21% to 30% congestion is 9.375%, ...

The drop probability scale supports values in the range 0-10% and the discrete values 25%, 50%, 75%, and 100%. Other values are silently truncated to the next lower value by the hardware.
Explicit Congestion Notification (ECN):

ECN capability is an end-to-end feedback mechanism. Both ends of the TCP connection must participate. When ECN is enabled, packets marked as ECN capable and selected for discard by WRED are marked CE and are not dropped. In cases of extreme congestion, ECN capable packets may be dropped.

Use the `show interfaces traffic` command to see color aware drops and congestion levels.

ECN capability can be enabled in Windows Server 2008 and later releases using the following command:

```
netsh interface tcp set global ecncapability=enabled
```

**N1500 Series Switches**

N1500 Series switches only support a simple RED capability. The N1500 Series switch does not support configuration of the maximum threshold nor can the threshold or drop probability be configured for non-TCP traffic.

Dell EMC Networking N1500 Series switches implement a simple Random Early Discard (RED) capability. Only the minimum threshold (min-thresh) and drop probability (drop-prob-scale) may be configured for the TCP colors green/yellow/red. The maximum threshold may not be configured nor can the threshold or drop probability be configured for non-TCP traffic. ECN capability is supported.

Simple RED may be enabled/disabled for any CoS queue on the Dell EMC Networking N1500 Series switches, however, the drop probability must be one of the values given below. The percentage before the dash indicates the actual drop probability. The number after the dash indicates the value entered in the drop-prob-scale parameter.

- 0.097%: 1
- 0.195%: 2
- 0.391%: 4
- 0.781%: 8
- 1.563%: 16
- 3.125%: 31
- 6.250%: 63
Examples
This example configures simple RED on an N1500 series switch. CoS queue 1 is globally configured for simple RED with a congestion threshold of 50% and a drop probability of 0.781% for green colored traffic.

```
console(config)# random-detect queue-parms 1 min-thresh 50 0 0 drop-prob-scale 8 0 0
console(config)# cos-queue random-detect 1
```

**random-detect exponential-weighting-constant**

Use the random-detect exponential-weighting-constant command to configure the decay in the calculation of the average queue size user for WRED on an interface or all interfaces.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

```
random-detect exponential-weighting-constant 0-15
no random-detect exponential-weighting-constant
```

- **0–15** — The weighting constant is used to smooth the calculation of the queue size using the following formula where the 0-15 value is N.

**Default Configuration**

The default value is 15. This value corresponds to maximum smoothing of the average queue size.

**Command Mode**

Global Configuration mode, Interface Configuration mode (physical and port-channel), Interface Range mode

**User Guidelines**

The exponential weighting constant configuration is global and applies to all WRED colors and all CoS queues. To use the instantaneous queue size in the calculation of WRED drops, set the weighting constant to 0. Larger values of N reduce the effect of instantaneous changes. To update the current queue
size to $\frac{1}{2}$ the difference between the previous size and the current instantaneous queue size, set the weighting constant to 1. To update the current queue size to $\frac{1}{4}$ the difference between the previous size and the current instantaneous queue size, set the weighting constant to 2, ....

The average queue size is calculated for each physical interface independently.

**redirect**

Use the `redirect` command in Policy-Class-Map Configuration mode to specify that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

NOTE: This command is not available on the N1500 Series switches.

**Syntax**

`redirect interface`

- `interface` — Specifies any valid interface. Interface is Ethernet port or port-channel (Range: po1-po32 or gi1/0/1-gi1/0/24)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Policy-Class-Map Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example shows how to redirect incoming packets to port Gi1/0/1.

```
console(config-policy-classmap)#redirect gi1/0/1
```
service-policy

Use the service-policy command in either Global Configuration mode (for all system interfaces) or Interface Configuration mode (for a specific interface) to attach a policy to an interface. To return to the system default, use the no form of this command.

NOTE: This command is not available on the N1500 Series switches.

Syntax

service-policy {in|out} policymapname

no service-policy {in|out} policymapname

- policymapname—Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string. (Range: 1–31 alphanumeric characters.)
- in—Apply the policy on ingress.
- out—Apply the policy on egress.

Default Configuration

No policies are applied by default.

Command Mode

Global Configuration mode (for all system interfaces)

Interface Configuration (Ethernet, Port-channel) mode (for a specific interface)

User Guidelines

This command applies a DiffServ policy to an interface and enables DiffServ on the interface. No separate interface administrative mode command for DiffServ is available. Use the policy-map command to configure the DiffServ policy. The service-policy direction must match the direction given for the policy map. DiffServ is enabled globally by default.

Ensure that no attributes within the policy definition exceed the capabilities of the interface. When a policy is attached to an interface successfully, any attempt to change the policy definition, such that it would result in a violation of the interface capabilities, causes the policy change attempt to
fail. Applying a policy globally applies the policy to all physical interfaces. The policy appears in the running-config as part of the individual interface configuration.

**Example**

The following example shows how to attach a service policy named “DELL” to all interfaces for packets ingressing the switch.

```
console(config)#service-policy in DELL
```

### show class-map

Use the `show class-map` command to display all configuration information for the specified class.

**Note:** This command is not available on the N1500 Series switches.

**Syntax**

```
show class-map [classname]
```

- `classname` — Specifies the valid name of an existing DiffServ class.
  (Range: 1–31 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays all the configuration information for the class named “Dell”.

```
console#show class-map
```
<table>
<thead>
<tr>
<th>Class Name</th>
<th>Type</th>
<th>ACL Identifier or Reference Class Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>cee</td>
<td>All</td>
<td>acl</td>
</tr>
<tr>
<td>ipv4</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>stop_http_class</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

```
console#show class-map ipv4

Class Name............................. ipv4
Class Type............................. All
Match Rule Count....................... 1

 Match Criteria                  Values
---------------------------------- --------------------------------------------
Source IP Address     2.2.2.2 (255.255.255.0)

console#show class-map stop_http_class

Class Name............................. stop_http_class
Class Type............................. Any
Match Rule Count....................... 2

 Match Criteria                  Values
---------------------------------- ----------------------------------
Source IP Address     2001:db8::/32
Source Layer 4 Port    80(http/www)
```

**show classofservice dot1p-mapping**

Use the **show classofservice dot1p-mapping** command to display the current IEEE 802.1p priority mapping to internal traffic classes for a specific interface.

**Syntax**

```
show classofservice dot1p-mapping [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
```

**Default Configuration**

By default, interfaces are configured to trust the IEEE 802.1p value in received packets and utilize the dot1p-mapping to assign packets to CoS queues.
**Layer 2 Switching Commands**

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
If the interface is specified, the IEEE 802.1p mapping table of the interface is displayed. If omitted, the global configuration settings are displayed.
The following table lists the parameters in the example and gives a description of each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Priority</td>
<td>The 802.1p user priority value.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>The traffic class internal queue identifier to which the user priority value is mapped.</td>
</tr>
</tbody>
</table>

**Example**
The following example displays the default 802.1p traffic class mapping and user priorities.

```
console# show classofservice dot1p-mapping
User Priority    Traffic Class
-------------    ---------------
0              1
1              0
2              0
3              1
4              2
5              2
6              3
7              3
```

**show classofservice ip-dscp-mapping**
Use the `show classofservice ip-dscp-mapping` command to display the current IP DSCP mapping to internal traffic classes for a specific interface.

**Syntax**
```
show classofservice ip-dscp-mapping
```
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
console#show classofservice ip-dscp-mapping

<table>
<thead>
<tr>
<th>IP DSCP</th>
<th>Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (be/cs0)</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8 (cs1)</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>10 (af11)</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>12 (af12)</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>14 (af13)</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>16 (cs2)</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>18 (af21)</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>20 (af22)</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>22 (af23)</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
</tr>
<tr>
<td>24 (cs3)</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>26 (af31)</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>1</td>
</tr>
</tbody>
</table>
show classofservice trust

Use the show classofservice trust command to display the current trust mode setting for a specific interface.


**Syntax**

```
show classofservice trust [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

If the interface is specified, the port trust mode of the interface is displayed. If omitted, the port trust mode for global configuration is shown.

**Example**

The following example displays the current trust mode settings for the specified port.

```
console#show classofservice trust gigabitethernet 1/0/2
Class of Service Trust Mode: Dot1P
```

**show diffserv**

Use the `show diffserv` command to display the DiffServ general information, which includes the current administrative mode setting as well as the current and maximum number of DiffServ components.

**NOTE:** On the N1500 Series switches, enable Simple RED since the hardware is not capable of Weighted RED.

**Syntax**

```
show diffserv
```

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the DiffServ information.

```
console#show diffserv
DiffServ Admin mode....................... Enable
Class Table Size Current/Max.............. 5 / 25
Class Rule Table Size Current/Max......... 6 / 150
Policy Table Size Current/Max............. 2 / 64
Policy Instance Table Size Current/Max... 2 / 640
Policy Attribute Table Size Current/Max.. 2 / 1920
Service Table Size Current/Max........... 26 / 214
```

show diffserv service interface

Use this command to display policy service information for the specified interface.

NOTE: This command is not available on the N1500 Series switches.

Syntax

```
show diffserv service interface \{interface-id\} \{in|out\}
```

-  interface-id—An Ethernet or port-channel identifier.
-  in—Show ingress policies.
-  out—Show egress policies.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes
**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show diffserv service interface gigabitethernet 1/0/1 in
```

DiffServ Admin Mode........................... Enable
Interface..................................... Gi1/0/1
Direction..................................... In
No policy is attached to this interface in this direction.

**show diffserv service brief**

Use the `show diffserv service brief` command to display all interfaces in the system to which a DiffServ policy has been attached.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

```
show diffserv service brief
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example shows how to display all interfaces in the system to which a DiffServ policy has been attached.

```
console(config)#show diffserv service brief
DiffServ Admin Mode........................... Enable
Interface Direction OperStatus Policy Name
------------------------------------------
```
show interfaces cos-queue

Use the show interfaces cos-queue command to display the class-of-service queue configuration for the specified interface.

Syntax

show interfaces cos-queue [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

If the interface is specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Examples

The following example displays the COS configuration with no unit/slot/port or port-channel parameter.

console#show interfaces cos-queue

Global Configuration
Interface Shaping Rate......................... 0

<table>
<thead>
<tr>
<th>Queue Id</th>
<th>Min. Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
</tbody>
</table>
This example displays the COS configuration for the specified interface Gi1/0/1.

```
console#show interfaces cos-queue gigabitethernet 1/0/1
Interface............................................. Gi1/0/1
Interface Shaping Rate............................. 0
```

<table>
<thead>
<tr>
<th>Queue Id</th>
<th>Min. Bandwidth</th>
<th>Scheduler Type</th>
<th>Queue Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>Weighted</td>
<td>Tail Drop</td>
</tr>
</tbody>
</table>

The following table lists the parameters in the examples and gives a description of each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The port of the interface. If displaying the global configuration, this output line is replaced with a global configuration indication.</td>
</tr>
<tr>
<td>Intf Shaping Rate</td>
<td>The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth values in effect for the interface. This value is a configured value.</td>
</tr>
<tr>
<td>Queue Mgmt Type</td>
<td>The queue depth management technique used for all queues on this interface.</td>
</tr>
<tr>
<td>Queue</td>
<td>An interface supports n queues numbered 0 to (n-1). The specific n value is platform-dependent. Internal egress queue of the interface; queues 0–6 are available.</td>
</tr>
</tbody>
</table>
show interfaces random-detect

Use the show interfaces random-detect command to display the global WRED policy or for an interface.

**Syntax**

```plaintext
show interfaces random-detect interface-id
```

- `interface-id`—Specify an optional interface type. Valid interfaces include physical ports and port channels.

**Default Configuration**

For the N1500, the default drop probability is 8 – 0.781% and the default minimum thresholds for Red/Yellow/Green colored packets are 40/30/20 percent respectively.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command displays the globally configured policy if no interface parameter is given. If an interface parameter is given, it displays the configured interface policy. The per CoS queue display for an interface displays the minimum and maximum thresholds, drop probability, and ECN capability per TCP packet color in the order: green, yellow, red, and non-TCP. Absent a metering policy (see police-simple, police-one-rate or police-two-
rate commands), all packets are colored green. Use the `show interfaces cos-queue` command to show the global or per interface scheduler type and queue management types.

The N1500 Series switch does not support configuration of the maximum threshold nor can the threshold or drop probability be configured for non-TCP traffic.

**Example**

**Example 1**

This example shows ECN enabled for green color packets on CoS queues 0 and 1.

```
console#show interfaces random-detect
```

Global Configuration

<table>
<thead>
<tr>
<th>Queue ID</th>
<th>Minimum Threshold</th>
<th>Maximum Threshold</th>
<th>Drop Probability</th>
<th>ECN Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>1/ 0/ 0/ 0</td>
</tr>
<tr>
<td>1</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>1/ 0/ 0/ 0</td>
</tr>
<tr>
<td>2</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>0/ 0/ 0/ 0</td>
</tr>
<tr>
<td>3</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>0/ 0/ 0/ 0</td>
</tr>
<tr>
<td>4</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>0/ 0/ 0/ 0</td>
</tr>
<tr>
<td>5</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>0/ 0/ 0/ 0</td>
</tr>
<tr>
<td>6</td>
<td>40/ 30/ 20</td>
<td>100/ 90/ 80/100</td>
<td>10/ 10/ 10/ 10</td>
<td>0/ 0/ 0/ 0</td>
</tr>
</tbody>
</table>

**Example 2**

This example show ECN enabled for green color packets on CoS queue 0 and on an N1500 Series switch:

```
console#show interfaces random-detect
```

Global Configuration

<table>
<thead>
<tr>
<th>Queue ID</th>
<th>Minimum Threshold</th>
<th>SRED Drop</th>
<th>ECN Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>1/ 0/ 0</td>
</tr>
<tr>
<td>1</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>1/ 0/ 0</td>
</tr>
<tr>
<td>2</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>0/ 0/ 0</td>
</tr>
<tr>
<td>3</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>0/ 0/ 0</td>
</tr>
<tr>
<td>4</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>0/ 0/ 0</td>
</tr>
<tr>
<td>5</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>0/ 0/ 0</td>
</tr>
<tr>
<td>6</td>
<td>40/ 30/ 20</td>
<td>8/ 8/ 8</td>
<td>0/ 0/ 0</td>
</tr>
</tbody>
</table>
**show policy-map**

Use the `show policy-map` command to display all configuration information for the specified policy.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.

**Syntax**

`show policy-map [policyname]`

- `policyname` — Specifies the name of a valid existing DiffServ policy.
  (Range: 1-31)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the DiffServ information.

```
console#show policy-map
Policy Name  Policy Type  Class Members
-----------  -----------  -------------
POLY1        xxx           DellClass
DELL         xxx            DellClass
```

**show policy-map interface**

Use the `show policy-map interface` command to display policy-oriented statistics information for the specified interface.

⚠️ **NOTE:** This command is not available on the N1500 Series switches.
**Syntax**

show policy-map interface {interface-id} {in|out}

- **interface-id**—An Ethernet or port-channel identifier.
- **in**—Show inbound service policies. The offered value indicates the number of packets received by the classifier.
- **out**—Show outbound service policies. The discarded value indicates the number of packets discarded by the policy.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the statistics information for port te1/0/1.

```
cconsole#show policy-map interface te1/0/1 in
Interface..................................... Te1/0/1
Operational Status............................ Down
Policy Name................................... DELL
Interface Summary:
Class Name.................................... Dell EMC Networking
In Offered Packets............................ 1003
In Discarded Packets.......................... 11
```

**show service-policy**

Use the `show service-policy` command to display a summary of policy-oriented statistics information for all interfaces.

**Syntax**

`show service-policy {in | out}`
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays a summary of policy-oriented statistics information.

```
console#show service-policy in
  Oper       Policy
  Intf  Stat  Name
  ------ ----- -------------------------------
  Gi1/0/1   Down  DELL
  Gi1/0/2   Down  DELL
  Gi1/0/3   Down  DELL
  Gi1/0/4   Down  DELL
  Gi1/0/5   Down  DELL
  Gi1/0/6   Down  DELL
  Gi1/0/7   Down  DELL
  Gi1/0/8   Down  DELL
  Gi1/0/9   Down  DELL
  Gi1/0/10  Down  DELL
```

traffic-shape
Use the traffic-shape command in Global Configuration mode and Interface Configuration mode to specify the maximum transmission bandwidth limit for the interface as a whole. To restore the default interface shaping rate value, use the no form of this command.

Syntax
```
traffic-shape bw kbps
no traffic-shape
```
Layer 2 Switching Commands

- bw — Maximum transmission bandwidth value expressed in Kbps.
  (Range: 64 - 4294967295)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode, Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**
Traffic shaping, also known as rate shaping, has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. This command implements a true egress shaper where bursts of traffic are buffered and smoothed. Shaping occurs if the average rate exceeds the configured limit or a burst exceeds 2% of the configured limit. Effectively, all CoS queues are configured with the configured rate limit in the scheduler.

Traffic shaping may cause congestion and packet loss if the aggregate ingress rate for an interface persistently exceeds the egress traffic shape rate.

**Example**
The following example rate limits interface gi1/0/1 to a maximum bandwidth of 1024 Kbps.

```
console(config-if-Gi1/0/1)#traffic-shape 1024 Kbps
```

**vlan priority**
Use the vlan priority command to assign a default VLAN priority tag for untagged frames ingressing an interface.

**Syntax**

```
vlan priority cos-value
```

- cos-value — A value ranging from 0-7.
Default Configuration
By default, untagged frames are processed with VLAN priority 0. The VLAN priority is mapped to a class of service value which determines the handling of the frame. Use the show interfaces detail command to display the configured priority. Use the show classofservice dot1p-mapping command to display the mapping of VLAN priorities to COS values.

Command Modes
Interface (physical) Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures the default VLAN priority to 1 for untagged frames ingressing interface Te1/0/1.

    console(config-if-Te1/0/1)#vlan priority 1
Spanning Tree Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Multiple Spanning Tree Protocol (MSTP) component complies with IEEE 802.1 by efficiently segregating VLAN traffic over separate interfaces for multiple instances of Spanning Tree. IEEE 802.1D, Spanning Tree and IEEE w, Rapid Spanning Tree are supported through the IEEE 802.1s implementation. The difference between the RSTP and STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations. The difference enables RSTP to rapidly transition to the Forwarding state and to suppress the Topology Change Notification PDUs, where possible.

A VLAN ID does not have to be preconfigured before mapping it to an MST instance.

Management of MSTP is compliant with the requirements of RFC5060.

The following features are supported by Dell EMC Networking MSTP:

STP Loop Guard - The Loop Guard feature is an enhancement of the Multiple Spanning Tree Protocol. Loop guard protects a network from forwarding loops induced by BPDU packet loss. It can be configured to prevent a blocked port from transitioning to the forwarding state when the port stops receiving BPDUs for some reason (such as a uni-directional link failure).

STP BPDU Guard - The STP BPDU guard allows the network administrator to enforce the STP domain borders and keep the active topology consistent and predictable. The switches behind the edge ports that have STP BPDU guard enabled are not able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation diagnostically disables a port that is configured with this option. Use the `spanning-tree bpdu-protection` command to enable BPDU guard.

STP Root Guard - The root guard ensures that the port on which root guard is enabled is the designated port. In a root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP BPDUs on a root guard enabled port, root guard moves this port to a root inconsistent STP state. This root inconsistent state is effectively equal to a listening state. No traffic is forwarded across this
port. In this way, the root guard enforces the position of the root bridge. In MSTP scenario the port may be designated in one of the instances while being alternate in the CIST, and so on. Root guard is a per port (not a per port per instance command) configuration so all the MSTP instances this port participates in should not be in root role.

**STP BPDU Filtering** - STP BPDU filtering applies to all operational edge ports. An Edge Port is supposed to be connected to hosts that typically do not generate BPDUs. Ports on which BDPU filtering is enabled will drop both transmitted and received BPDUs. As a result, loops may be formed on ports for which BPDU filtering is enabled.

**STP BPDU Flooding** - STP BPDU flooding feature applies to an STP disabled switch. To enable BPDU flooding on a port, STP must be disabled on the switch administratively. When this feature is enabled on the switch, it floods all the ports which have the BPDU flood feature enabled.

**BPDU Storm Protection** - If STP BPDUs are received at a rate of 15 pps or greater for 3 consecutive seconds on a port, the port will be diagnostically disabled. A message of the following form is logged:

```
<188> MAY 04 09:45:23 10.10.10.10-1 DOT1S[276072720]: dot1s_ih.c(1587)
15855515 %% Diagnostically disabling interface 2/0/41
```

Use the `no shut` command to return the port to service.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear spanning-tree detected-protocols</th>
<th>spanning-tree backbonefast</th>
<th>spanning-tree mode</th>
<th>spanning-tree priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit (mst)</td>
<td>spanning-tree bpdu flooding</td>
<td>spanning-tree mst configuration</td>
<td>spanning-tree tcnguard</td>
</tr>
<tr>
<td>instance (mst)</td>
<td>spanning-tree bpdu-protection</td>
<td>spanning-tree mst cost</td>
<td>spanning-tree transmit hold-count</td>
</tr>
<tr>
<td>name (MST)</td>
<td>spanning-tree cost</td>
<td>spanning-tree mst port-priority</td>
<td>spanning-tree uplinkfast</td>
</tr>
<tr>
<td>revision (mst)</td>
<td>spanning-tree disable</td>
<td>spanning-tree mst priority</td>
<td>spanning-tree vlan</td>
</tr>
</tbody>
</table>
Use the `clear spanning-tree detected-protocols` command to restart the protocol migration process (forces the renegotiation with neighboring switches) on all interfaces or on the specified interface.

**Syntax**

`clear spanning-tree detected-protocols [ interface-id ]`

- `interface-id`—An Ethernet or port channel interface identifier

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This feature is used only when working in RSTP or MSTP mode.

**Example**

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on Gi1/0/1.
exit (mst)

Use the `exit` command in MST mode to exit the MST configuration mode and apply all configuration changes.

**Syntax**

```
exit
```

**Default Configuration**

MST configuration.

**Command Mode**

MST mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example shows how to exit the MST configuration mode and save changes.

```
console(config)#spanning-tree mst configuration
console(config-mst)#exit
```

instance (mst)

Use the `instance` command in MST mode to map VLANS to an MST instance.

**Syntax**

```
instance instance-id {add | remove} vlan vlan-list
```

- `instance-ID` — ID of the MST instance. (Range: 1-4094)
- `vlan-list` — VLANS to be added to the existing MST instance. To specify a range of VLANS, use a hyphen. To specify a series of VLANS, use a comma. (Range: 1-4094)
**Default Configuration**

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

**Command Mode**

MST mode

**User Guidelines**

Before mapping VLANs to an instance use the `spanning-tree mst enable` command to enable the instance.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same configuration name.

Dell EMC Networking MSTP supports mapping of VLANs to MST instances, even though the underlying VLAN may not be defined on the switch. Traffic received on VLANs not defined on the port received is dropped.

For interoperability purposes, VLAN 4094 may be mapped to an MSTI, however, VLAN 4094 is reserved internally and may not be used to forward traffic.

**Example**

The following example maps the entire range of VLANs to MST instances (MST instance 0 is mapped to VLAN 1 by default). Additionally, two 10G ports have some, but not all, of the VLANs mapped to MST instances.

```console
console(config)#spanning-tree mode mst
console(config)#spanning-tree mst 1 priority 8192
console(config)#spanning-tree mst 2 priority 28672
console(config)#spanning-tree mst configuration
console(config-mst)#instance 1 add vlan 2-199
console(config-mst)#instance 1 add vlan 350
console(config-mst)#instance 1 add vlan 400-449
console(config-mst)#instance 1 add vlan 500-1999
console(config-mst)#instance 1 add vlan 2200-2499
console(config-mst)#instance 1 add vlan 2600-2799
```
console(config-mst)#instance 1 add vlan 3000-4093
console(config-mst)#instance 2 add vlan 200-349
console(config-mst)#instance 2 add vlan 351-399
console(config-mst)#instance 2 add vlan 450-499
console(config-mst)#instance 2 add vlan 2000-2199
console(config-mst)#instance 2 add vlan 2500-2599
console(config-mst)#instance 2 add vlan 2800-2999
console(config-mst)#exit
console(config)#interface te1/1/1
console(config-if-Te1/1/1)#switchport mode trunk
console(config-if-Te1/1/1)#switchport trunk allowed vlan add 2-150
console(config-if-Te1/1/1)#spanning-tree mst 1 port-priority 16
console(config-if-Te1/1/1)#interface te1/1/2
console(config-if-Te1/1/2)#switchport mode trunk
console(config-if-Te1/1/2)#switchport trunk allowed vlan add 200-349
console(config-if-Te1/1/2)#spanning-tree mst 2 port-priority 16
console(config-if-Te1/1/2)#exit

name (MST)

Use the name command in MST mode to define the region name. To return to the default setting, use the no form of this command.

Syntax

name string
  • string — Case sensitive MST configuration name. (Range: 1-32 characters)

Default Configuration

Bridge address.

Command Mode

MST mode

User Guidelines

When configuring the switch in MSTP mode, be sure to configure the MST region name. For multiple switches to become members of the same region, the configuration name, the configuration revision and mapping of VLANs to MSTIs must be identical.
**Example**
The following example sets the configuration name to “region1”.

```
console(config)#spanning-tree mst configuration
console(config-mst)#name region1
```

**revision (mst)**

Use the `revision` command in MST mode to identify the configuration revision number. To return to the default setting, use the `no` form of this command.

**Syntax**

```
revision version
no revision
```

- version — Configuration revision number. (Range: 0-65535)

**Default Configuration**

Revision number is 0.

**Command Mode**

MST mode

**User Guidelines**

When configuring the switch in MSTP mode, be sure to configure the MST region name. For multiple switches to become members of the same region, the configuration name, the configuration revision and mapping of VLANs to MSTIs must be identical.

**Example**

The following example sets the configuration revision to 1.

```
console(config)#spanning-tree mst configuration
console(config-mst)#revision 1
```
show spanning-tree

Use the show spanning-tree command to display the spanning-tree configuration.

Syntax

show spanning-tree [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}] [instance instance-id]

show spanning-tree [detail] [active | blockedports] | [instance instance-id]

show spanning-tree mst-configuration

show spanning-tree {uplinkfast | backbonefast}

• detail—Displays detailed information.
• active—Displays active ports only.
• blockedports—Displays blocked ports only.
• mst-configuration—Displays the MST configuration identifier.
• instance-id—ID of the spanning tree instance.
• uplinkfast—Displays Direct Link Rapid Convergence information.
• backbonefast—Displays Indirect Link Rapid Convergence information.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Command History

Modified in version 6.5 firmware.
Examples

The following examples display spanning-tree information. MST information is shown in this form of the command regardless of the spanning tree mode.

```
console#show spanning-tree
Spanning Tree: Enabled
Mode: rstp
BPDU Flooding: Disabled
Portfast BPDU Filtering: Enabled
Portfast BPDU Guard: Disabled
CST Regional Root: 80:00:00:1E:C9:AA:AD:1B
Regional Root Path Cost: 0
ROOT ID
Priority 32768
Address 0010.1882.1C53
Path Cost 20000
Root Port Gi1/0/1
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec TxHoldCount 6 sec
Bridge ID
Priority 32768
Address 001E.C9AA.AD1B
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name   State   Prio.Nbr   Cost      Sts  Role  Restricted
------ -------- --------- --------- ---- ----- ----------
Gi1/0/1 Enabled 128.1     20000     FWD  Root  No
Gi1/0/2 Enabled 128.2     0         DIS  Disb  No
Gi1/0/3 Enabled 128.3     0         DIS  Disb  No
Gi1/0/4 Enabled 128.4     0         DIS  Disb  No
```

```
console#show spanning-tree gi1/0/1
Port: Gi1/0/1   Enabled
State: Forwarding                                Role: Designated
Port ID: 128.1                                   Port Cost: 20000
Port Fast: No                                    Root Protection: No
Designated Bridge Priority: 32768                Address: 001E.C9DE.D447
Designated Port ID: 128.1                        Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47        Root Guard............................. False
Root Guard........................................ Root Protection: No
Loop Guard....................................... False
Auto Portfast.................................... True
BPDU Filter Mode................................. Disabled
Time Since Counters Last Cleared................. 0d0h2m46s
```
BPDUs: Sent: 74, Received: 0

console#show spanning-tree detail
Spanning Tree: Enabled    (BPDU Flooding: Disabled)
Mode: rstp Portfast BPDU Filtering: Disabled
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
Regional Root Path Cost: 0
  Address 80:00:00:1E:C9:DE:D4:47
  This Switch is the Root.
  Hello Time: 2s Max Age: 20s Forward Delay: 15s Transmit Hold
  Count: 6s
  Bridge Max Hops: 20
Number of topology changes: 1 Last Change Occurred: 0d0h3m6s ago
Times: Hold: 6, Hello: 2, Max Age: 20, Forward Delay: 15
Port: Gi1/0/1 Enabled
State: Forwarding        Role: Designated
Port ID: 128.1           Port Cost: 20000
Root Protection: No
Designated Bridge Priority: 32768
Designated Port ID: 128.1
Designated Port Priority: 32768
Designated Port ID: 128.1
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
CST Port Cost: 0
BPDUs: Sent: 83, Received: 0
Port: Gi1/0/2 Enabled
State: Forwarding        Role: Designated
Port ID: 128.2           Port Cost: 20000
Root Protection: No
Designated Bridge Priority: 32768 Address: 001E.C9DE.D447
Designated Port ID: 128.2
Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
CST Port Cost: 0
BPDUs: Sent: 84, Received: 2
Port: Gi1/0/3 Enabled
State: Disabled          Role: Disabled
Port ID: 128.3           Port Cost: 0
Root Protection: No
Designated Bridge Priority: 32768 Address: 001E.C9DE.D447
Designated Port ID: 0.0
Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
CST Port Cost: 0
BPDUs: Sent: 0, Received: 0

console#show spanning-tree detail active
Spanning Tree: Enabled    (BPDU Flooding: Disabled)
Mode: rstp Portfast BPDU Filtering: Disabled
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
Regional Root Path Cost: 0
ROOT ID
Address  
80:00:00:1E:C9:DE:D4:47
This Switch is the Root.
Hello Time: 2s Max Age: 20s Forward Delay: 15s Transmit Hold Count: 6s
Bridge Max Hops: 20
Number of topology changes: 1 Last Change Occurred: 0d0h4m13s ago
Times: Hold: 6, Hello: 2, Max Age: 20, Forward Delay: 15
Port: Gi1/0/1 Enabled
State: Forwarding  Role: Designated
Port ID: 128.1  Port Cost: 20000
Root Protection: No
Designated Bridge Priority: 32768  Address: 001E.C9DE.D447
Designated Port ID: 128.1  Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47  CST Port Cost: 0
BPDUs: Sent: 112, Received: 0
Port: Gi1/0/2 Enabled
State: Forwarding  Role: Designated
Port ID: 128.2  Port Cost: 20000
Root Protection: No
Designated Bridge Priority: 32768  Address: 001E.C9DE.D447
Designated Port ID: 128.2  Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47  CST Port Cost: 0
BPDUs: Sent: 113, Received: 2
Port: Te1/0/1 Enabled
State: Forwarding  Role: Designated
Port ID: 128.49  Port Cost: 2000
Root Protection: No
Designated Bridge Priority: 32768  Address: 001E.C9DE.D447
Designated Port ID: 128.49  Designated Path Cost: 0
CST Regional Root: 80:00:00:1E:C9:DE:D4:47  CST Port Cost: 0
BPDUs: Sent: 113, Received: 1

console#show spanning-tree blockedports
Spanning Tree: Enabled (BPDU Flooding: Disabled) Mode: rstp
CST Regional Root: 80:00:00:1E:C9:DE:D4:47
Regional Root Path Cost: 0
##### MST 0 Vlan Mapped: 1-10
ROOT ID

Priority 32768
Address 001E.C9DE.D447
This Switch is the Root.
Hello Time: 2s Max Age: 20s Forward Delay: 15s

Interfaces
<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/2</td>
<td>Enabled</td>
<td>128.50</td>
<td>2000</td>
<td>DSC</td>
<td>Bkup</td>
<td>No</td>
</tr>
</tbody>
</table>
console(config)#show spanning-tree uplinkfast
Directlink rapid convergence is enabled
BPDU update rate : 150 packets/sec
Directlink rapid convergence Statistics
---------------------
Directlink rapid convergence transitions (all VLANs).. 0
Proxy multicast addresses transmitted (all VLANs)..... 0
Name                             Interface list
---------------                  ------------------------------------
VLAN0001                         Gi1/0/2(fwd)
VLAN0002
VLAN0003
VLAN0004
VLAN0005
VLAN0006
VLAN0007
VLAN0008
VLAN0009
VLAN0010

console(config)#show spanning-tree backbonefast
Indirectlink rapid convergence is enabled
Indirectlink rapid convergence Statistics
---------------------
Transitions via indirectlink rapid convergence.. 0
Inferior BPDUs received (all VLANs)............ 7
RLQ request PDUs received (all VLANs)............ 0
RLQ response PDUs received (all VLANs)......... 0
RLQ request PDUs sent (all VLANs)............... 0
RLQ response PDUs sent (all VLANs).............. 0

This example shows spanning-tree configured in mstp mode. Output is shown for each VLAN that is a member of an MST domain.

    console(config-mst)#show spanning-tree active

Spanning Tree: Enabled   (BPDU Flooding: Disabled)
Mode: rstp Portfast BPDU Filtering: Disabled
CST Regional Root:       80:00:00:1E:C8:DE:D4:47
Regional Root Path Cost: 0
Layer 2 Switching Commands

### MST 0 Vlan Mapped: 1

**ROOT ID**

- **Priority**: 32768
- **Address**: 001E.C9DE.D447
- This Switch is the Root.
- **Hello Time**: 2s Max Age: 20s Forward Delay: 15s

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>0</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>0</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/1</td>
<td>Enabled</td>
<td>128.49</td>
<td>0</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/2</td>
<td>Enabled</td>
<td>128.50</td>
<td>0</td>
<td>DSC</td>
<td>Bkup</td>
<td>No</td>
</tr>
</tbody>
</table>

### MST 1 Vlan Mapped: 2

**ROOT ID**

- **Priority**: 32768
- **Address**: 001E.C9DE.D447
- This Switch is the Root.
- **Hello Time**: 2s Max Age: 20s Forward Delay: 15s

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
</tbody>
</table>

### MST 2 Vlan Mapped: 3-5

**ROOT ID**

- **Priority**: 4096
- **Address**: 001E.C9DE.D447
- This Switch is the Root.
- **Hello Time**: 2s Max Age: 20s Forward Delay: 15s

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
</tbody>
</table>

### MST 3 Vlan Mapped: 6-10

**ROOT ID**

- **Priority**: 32768
- **Address**: 001E.C9DE.D447
- This Switch is the Root.
- **Hello Time**: 2s Max Age: 20s Forward Delay: 15s
Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
</tbody>
</table>

console(config)#show spanning-tree instance 2

Spanning Tree: Enabled    BPDU Flooding: Disabled
Mode: mstp Portfast BPDU Filtering: Disabled
CST Regional Root:        80:00:00:1E:C9:DE:D4:47
Regional Root Path Cost:  0

##### MST 2 Vlan Mapped: 3-5
ROOT ID
- Priority: 4096
- Address: 001E.C9DE.D447
- Path Cost: 0
- Root Port:

Bridge ID
- Priority: 4096
- Address: 001E.C9DE.D447
- Hello Time: 2s Max Age: 20s Forward Delay: 15s Transmit Hold
- Count: 6s

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>0</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>0</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enabled</td>
<td>128.3</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Enabled</td>
<td>128.5</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Enabled</td>
<td>128.6</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>Enabled</td>
<td>128.7</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>Enabled</td>
<td>128.8</td>
<td>0</td>
<td>DIS</td>
<td>Disb</td>
<td>No</td>
</tr>
</tbody>
</table>

This example shows spanning-tree configured in rstp mode. Output is shown for each interface.

console(config)#show spanning-tree active

Spanning Tree: Enabled    (BPDU Flooding: Disabled)
Mode: rstp Portfast BPDU Filtering: Disabled
CST Regional Root:        80:00:00:1E:C9:DE:D4:47
Regional Root Path Cost:  0

##### MST 0 Vlan Mapped: 1-10
ROOT ID

Priority        32768
Address         001E.C9DE.D447
This Switch is the Root.
Hello Time: 2s Max Age: 20s Forward Delay: 15s

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>RestrictedPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/1</td>
<td>Enabled</td>
<td>128.49</td>
<td>2000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>Te1/0/2</td>
<td>Enabled</td>
<td>128.50</td>
<td>2000</td>
<td>DSC</td>
<td>Bkup</td>
<td>No</td>
</tr>
</tbody>
</table>

This example shows spanning-tree configured in rapid-pvst mode. Output is shown for each VLAN that is actively running a spanning tree instance.

console(config)#show spanning-tree active
Spanning-tree enabled protocol rpvst
VLAN  1
RootID  Priority        32768
Address         F8B1.562B.A1D6
Cost            20000
Port            2(Gi1/0/2)
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
Address         001E.C9DE.D447
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time   300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- ------- ------------- -----------
Gi1/0/1   Enabled   128.1     20000   Forwarding    Designated
Gi1/0/2   Enabled   128.2     20000   Forwarding    Root
Te1/0/1   Enabled   128.49    2000    Forwarding    Designated
Te1/0/2   Enabled   128.50    2000    Discarding    Backup

VLAN  2
RootID  Priority        32770
Address         001E.C9DE.D447
Cost            0
Port            This switch is the root
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
BridgeID  Priority        32770 (priority 32768 sys-id-ext 2)
Address         001E.C9DE.D447
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time   300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- ------- ------------- ---------
show spanning-tree summary

Use the `show spanning-tree summary` command to display spanning tree settings and parameters for the switch.

**Syntax**

`show spanning-tree summary`

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning Tree Admin Mode</td>
<td>Enabled or disabled</td>
</tr>
<tr>
<td>Spanning Tree Version</td>
<td>Version of currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the mode parameter.</td>
</tr>
<tr>
<td>BPDU Protection Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>BPDU Filter Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>BPDU Flooding Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>IndirectLink Rapid</td>
<td>Backbone-fast for RSTP-PV is enabled or disabled.</td>
</tr>
<tr>
<td>Convergence</td>
<td></td>
</tr>
<tr>
<td>DirectLink Rapid</td>
<td>Enables/Disables DRC by setting switch priority to 49152.</td>
</tr>
<tr>
<td>Convergence</td>
<td></td>
</tr>
</tbody>
</table>
### Example

```
console#show spanning-tree summary
Spanning Tree Admin Mode.......... Enabled
Spanning Tree Version............. IEEE 802.1w
BPDU Guard Mode................... Disabled
BPDU Flood Mode................... Disabled
IndirectLink Rapid Convergence.... Disabled
DirectLink Rapid Convergence...... Disabled
BPDU Filter Mode.................. Disabled
Configuration Name.............. 14-18-77-0C-9D-D8
Configuration Revision Level...... 0
Configuration Digest Key.......... 0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
```

### show spanning-tree vlan

Use the `show spanning-tree vlan` command to display spanning tree information per VLAN and also list out the port roles and states as well as port cost.

**Syntax**

```
show spanning-tree vlan { vlan-list | all }
```

- `vlan-list` — A list of VLANs or VLAN ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form X-Y where X and Y are valid VLAN identifiers and X < Y.
- **all**—Show all VLANs.

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Privileged Exec and above

**User Guidelines**

There are no user guidelines for this command.

**Example**

```console
console(config)#show spanning-tree vlan 2
VLAN    2
Spanning Tree: Enabled Mode: rapid-pvst
RootID    Priority        32770
          Address         001E.C9DE.D447
          Cost            0
          Port            This switch is the root
          Hello Time: 2s Max Age: 20s Forward Delay: 15s
BridgeID  Priority        32770 (priority 32768 sys-id-ext 2)
          Address         001E.C9DE.D447
          Hello Time: 2s Max Age: 20s Forward Delay: 15s
          Aging Time 300 sec
Interface Role       Sts           Cost      Prio.Nbr
--------- ---------- ------------- --------- --------
Gi1/0/1   Designated Forwarding 20000     128.1
Gi1/0/2   Designated Forwarding 20000     128.2
```

**spanning-tree**

Use the `spanning-tree` command in Global Configuration mode to enable spanning-tree functionality. To disable spanning-tree functionality, use the `no` form of this command.

**Syntax**

- `spanning-tree`
- `no spanning-tree`
Default Configuration
Spanning-tree is enabled.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example enables spanning-tree functionality.

```
console(config)#spanning-tree
```

```spanning-tree auto-portfast```

Use the `spanning-tree auto-portfast` command to set the port to auto portfast mode. This enables the port to become a portfast port if it does not see any BPDUs for 3 seconds after a link up event. Use the `no` form of this command to disable auto portfast mode.

Syntax
- `spanning-tree auto-portfast`
- `no spanning-tree auto-portfast`

Default Configuration
Auto portfast mode is enabled by default.

Command Mode
Interface Configuration (Ethernet, Port Channel) mode

User Guidelines
There are no user guidelines for this command.
Example
The following example enables spanning-tree functionality on Gigabit ethernet interface 4/0/1.

console#config
console(config)#interface gigabitethernet 4/0/1
console(config-if-4/0/1)#spanning-tree auto-portfast

spanning-tree backbonefast
Use the spanning-tree backbonefast command to enable the detection of indirect link failures and accelerate spanning tree convergence on STP-PV/RSTP-PV configured switches using Indirect Link Rapid Convergence (IRC). IRC accelerates finding an alternative path when an indirect link to the root port goes down. Use the no form of the command to disable the IRC feature.

Syntax
spanning-tree backbonefast
no spanning-tree backbonefast

Default Configuration
This command has no default configuration.

Command Modes
Global Configuration Mode

User Guidelines
IRC can be configured even if the switch is configured for MST(RSTP) or RSTP-PV mode. It only has an effect when the switch is configured for STP-PV mode.

If an IRC-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternative (blocked) paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.
Example

console(config)#spanning-tree backbonefast

**spanning-tree bpdu flooding**

The `spanning-tree bpdu flooding` command allows flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports. Use the “no” form of the command to disable flooding.

**Syntax**

```plaintext
spanning-tree bpdu flooding
no spanning-tree bpdu flooding
```

**Default Configuration**

This feature is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

There are no user guidelines for this command.

Example

```plaintext
console#spanning-tree bpdu flooding
```

**spanning-tree bpdu-protection**

Use the `spanning-tree bpdu-protection` command in Global Configuration mode to enable BPDU guard on a switch. Use the `no` form of this command to resume the default status of BPDU guard function.

**Syntax**

```plaintext
spanning-tree bpdu-protection
no spanning-tree bpdu-protection
```
**Default Configuration**

BPDU guard is not enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

The administrator should ensure that interfaces on which BDPU guard is enabled are configured as edge ports. To configure an interface as an edge port, use the `spanning-tree portfast` command.

An edge port is generally connected to a user terminal (such as a desktop computer) or file server directly and is configured as an edge port to implement a fast transition to the forwarding state. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree topology, which may cause network topology flapping. In normal cases, edge ports do not receive any BPDU packets. However, an attacker may forge BPDU packets to maliciously disrupt the switch and cause network flapping.

Dell spanning-tree provides a BPDU guard function against such attacks. If an interface enabled for BPDU guard receives a BPDU packet, the interface is diagnostically disabled and a message is written to the log. The port may be re-enabled using the `no shutdown` command after disconnecting the offending device from the interface.

**Example**

The following example enables BPDU protection.

```
console(config)#spanning-tree bpdu-protection
```

**spanning-tree cost**

Use the `spanning-tree cost` command in Interface Configuration mode to configure the externally advertised spanning-tree path cost for a port. To return to the default port path cost, use the `no` form of this command.

The path cost is used in the selection of an interface for the forwarding or blocking states. Use the `no` form of the command to automatically select the path cost based upon the speed of the interface.
**Syntax**

```
spanning-tree [vlan vlan-list] cost cost
no spanning-tree cost
```

- **cost** — The port path cost.

**Default Configuration**

The default cost value (0) causes the switch to select the path cost based on the link speed.

- **40G Port path cost** — 1400
- **10G Port path cost** — 2000
- **1000 Mbps (giga)** — 20,000
- **100 Mbps** — 200,000
- **10 Mbps** — 2,000,000
- **Port Channel**—200,000,000 divided by the sum of the unidirectional link speed (in Mbps) of each active member multiplied by 10 per section 13.6.1 of IEEE 802.1s.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

Dell EMC Networking spanning tree uses long values for spanning tree costs. The range for path cost for a port is 0-200,000,000. The range for path cost for a VLAN is 1-200,000,000. Use the `no` form of the command to calculate the cost based on the interface speed. A zero path cost causes the switch to calculate the path cost based upon the speed of the interface.

If the VLAN parameter is given, the path cost is configured only for the selected VLANs (applies only when pvst or rapid-pvst mode is selected). Configuration without the VLAN parameter configures the interface path cost for STP, RSTP, and the MSTP common instance.
If an interface is configured with both the `spanning-tree vlan vlan-id cost` command and the `spanning-tree cost` command, the `spanning-tree vlan vlan-id cost` cost value is used in the spanning tree calculation for RSTP, STP, and MST. Use the `spanning-tree vlan cost` command to change the cost for RSTP-PV and STP-PV.

**Example**

The following example configures the external path cost to be 8192 for VLANs 12, 13, 24, 25, and 26.

```
console(config-if-Gi1/0/1)#spanning-tree vlan 12,13,24-26 cost 8192
```

**spanning-tree disable**

Use the `spanning-tree disable` command in Interface Configuration mode to disable spanning-tree on a specific port. To enable spanning-tree on a port, use the `no` form of this command.

**Syntax**

```
spanning-tree disable
no spanning-tree disable
```

**Default Configuration**

By default, all ports are enabled for spanning-tree.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example disables spanning-tree on Gi1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)#spanning-tree disable
```
**spanning-tree forward-time**

Use the `spanning-tree forward-time` command in Global Configuration mode to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

To reset the default forward time, use the `no` form of this command.

**Syntax**

```plaintext
spanning-tree forward-time seconds
no spanning-tree forward-time

- seconds — Time in seconds. (Range: 4–30)
```

**Default Configuration**

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

**Command Mode**

Global Configuration mode.

**User Guidelines**

When configuring the Forward-Time the following relationship should be satisfied:

\[ 2^*(\text{Forward-Time} - 1) \geq \text{Max-Age} \]

**Example**

The following example configures spanning-tree bridge forward time to 25 seconds.

```
colosse(config)#spanning-tree forward-time 25
```
spanning-tree guard
The spanning-tree guard command selects whether loop guard or root guard is enabled on an interface. If neither is enabled, the port operates in accordance with the multiple spanning tree protocol. Use the “no” form of this command to disable loop guard or root guard on the interface.

Syntax
spanning-tree guard {root | loop | none}
  • root — Enables root guard.
  • loop — Enables loop guard
  • none — Disables root and loop guard.

Default Configuration
Neither root nor loop guard is enabled.

Command Mode
Interface Configuration (Ethernet, Port Channel) mode.

User Guidelines
There are no user guidelines for this command.

Example
The following example disables spanning-tree guard functionality on Gigabit ethernet interface 4/0/1.

```
crash(config)#interface gigabitethernet 4/0/1
console(config-if-4/0/1)#spanning-tree guard none
```

spanning-tree loopguard
Use the spanning-tree loopguard command to enable loop guard on all ports. Use the “no” form of this command to disable loop guard on all ports.

Syntax
spanning-tree loopguard default
no spanning-tree loopguard default

**Default Configuration**
Loop guard is disabled by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example enables spanning-tree loopguard functionality on all ports.

```
console(config)#spanning-tree loopguard default
```

### spanning-tree max-age

Use the `spanning-tree max-age` command in Global Configuration mode to configure the spanning-tree bridge maximum age. To reset the default maximum age, use the `no` form of this command.

**Syntax**

```
spanning-tree max-age seconds
no spanning-tree max-age
```

- **seconds** - Time in seconds. (Range: 6–40)

**Default Configuration**
The default max-age for IEEE STP is 20 seconds.

**Command Mode**
Global Configuration mode
User Guidelines
When configuring the Max-Age the following relationships should be satisfied:

\[ 2^*(Forward-Time - 1) \geq Max-Age \]
\[ Max-Age \geq 2^*(Hello-Time + 1) \]

Example
The following example configures the spanning-tree bridge maximum-age to 10 seconds.

console(config)#spanning-tree max-age 10

spanning-tree max-hops
Use the spanning-tree max-hops command to set the MSTP Max Hops parameter to a new value for the common and internal spanning tree. Use the “no” form of this command to reset the Max Hops to the default.

Syntax
spanning-tree max-hops hops
no spanning-tree max-hops

• hops — The maximum number of hops to use (Range: 6 to 40).

Default Configuration
The maximum number of hops is 20 by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)#spanning-tree max-hops 32
**spanning-tree mode**

Use the `spanning-tree mode` command in Global Configuration mode to configure the spanning-tree protocol. To return to the default configuration, use the `no spanning-tree` form of this command.

**Syntax**

```
spanning-tree mode {stp | rstp | mst | pvst | rapid-pvst}
```

- `stp` — Spanning Tree Protocol (STP) is enabled.
- `rstp` — Rapid Spanning Tree Protocol (RSTP) is enabled.
- `mst` — Multiple Spanning Tree Protocol (MSTP) is enabled.
- `pvst` — Spanning-tree operates in STP-PV mode.
- `rapid-pvst` — Spanning-tree operates in RSTP-PV mode.

**Default Configuration**

Rapid Spanning Tree Protocol (RSTP) is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

In RSTP mode, the switch uses STP when the neighbor switch is using STP. In MSTP mode, the switch uses RSTP when the neighbor switch is using RSTP and uses STP when the neighbor switch is using STP.

Only one of STP, RSTP, MSTP (RSTP), STP-PV or RSTP-PV can be enabled on a switch. This command stops all spanning-tree instances in the current mode and enables spanning-tree per VLAN in the new mode. By default, RSTP is enabled.

If configuring the switch to MSTP mode, be sure to configure the MST region name. For multiple switches to become members of the same region, the configuration name, the configuration revision and mapping of VLANs to MSTIs must be identical.

In the STP-PV or RSTP-PV modes, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).
RSTP-PV maintains independent spanning tree information about each configured VLAN. RSTP-PV uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per VLAN basis. This allows a trunk port to be forwarding for some VLANs and blocked on other VLANs.

RSTP-PV extends the IEEE 802.1w standard. It supports faster convergence than IEEE 802.1D. RSTP-PV is compatible with IEEE 802.1D spanning tree. RSTP-PV sends BPDUs on all ports instead of only the root bridge sending BPDUs and supports the discarding, learning, and forwarding states.

When the mode is changed to rapid-pvst, version 0 STP BPDUs are no longer transmitted and version 2 RSTP-PV BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, RSTP-PV reverts to sending version 0 BPDUs.

RSTP-PV embeds support for STP-PV Indirect Link Rapid Convergence and Direct Link Rapid Convergence. There is no provision to enable or disable these features in RSTP-PV.

**Example**

The following example configures the spanning-tree protocol to MSTP.

```console
console(config)#spanning-tree mode mst
```

**spanning-tree mst configuration**

Use the `spanning-tree mst configuration` command in Global Configuration mode to enable configuring an MST region by entering the multiple spanning-tree (MST) mode.

**Syntax**

`spanning-tree mst configuration`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode
User Guidelines

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number and the same name.

Example

The following example configures an MST region.

```
console (config)#spanning-tree mst configuration
console (config-mst)#instance 1 add vlan 10-20
console (config-mst)#name region1
console (config-mst)#revision 1
```

spanning-tree mst cost

Use the `spanning-tree mst cost` command in Interface Configuration mode to configure the internal path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default port path cost, use the `no` form of this command.

Syntax

```
spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost
```

- `instance-ID` — ID of the spanning-tree instance. (Range: 1-4094)
- `cost` — The port path cost. (Range: 0–200,000,000)

Default Configuration

The default cost is 0, which signifies that the cost will be automatically calculated based on port speed.

The default configuration is:

- Ethernet (10 Mbps) — 2,000,000
- Fast Ethernet (100 Mbps) — 200,000
- Gigabit Ethernet (1000 Mbps) — 20,000
- Port-Channel — 20,000
**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

Use the `spanning-tree cost` command to configure MST instance 0 (the common spanning tree instance). Use the `show spanning-tree active` command to display the spanning tree costs.

**Example**

The following example configures the MSTP instance 1 path cost for Gigabit Ethernet interface 1/0/9 to 4.

```
console(config)#interface gigabitethernet 1/0/9
console(config-if-Gi1/0/9)#spanning-tree mst 1 cost 4
```

**spanning-tree mst port-priority**

Use the `spanning-tree mst port-priority` command in Interface Configuration mode to configure port priority. To return to the default port priority, use the `no` form of this command.

**Syntax**

```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

- **instance-id**—ID of the spanning-tree instance. (Range: 1-4094)
- **priority**—The port priority. (Range: 0-240 in multiples of 16.)

**Default Configuration**

The default port-priority for IEEE STP is 128. The default priority for a port-channel is 96.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode
**User Guidelines**

The priority will be set to the nearest multiple of 4096 if not an exact multiple of 4096.

**Example**

The following example configures the port priority of Gigabit Ethernet interface 1/0/5 to 144.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if)#spanning-tree mst 1 port-priority 144
```

**spanning-tree mst priority**

Use the `spanning-tree mst priority` command in Global Configuration mode to set the switch priority for the specified spanning-tree instance. To return to the default setting, use the `no` form of this command.

**Syntax**

```
spanning-tree mst instance-id priority priority
no spanning-tree mst instance-id priority
```

- **instance-id**—ID of the spanning-tree instance. (Range: 1-4094)
- **priority**—Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0-61440)

**Default Configuration**

The default bridge priority for IEEE STP is 32768.

**Command Mode**

Global Configuration mode

**User Guidelines**

The priority value must be a multiple of 4096. The priority will be set to the nearest multiple of 4096 if not an exact multiple of 4096.
Bridge priority configuration is given preference over the root primary/secondary configuration. Root primary/secondary configuration is given preference over the DRC configuration.

The switch with the lowest priority is selected as the root of the spanning tree.

**Example**

The following example configures the spanning tree priority of instance 1 to 4096.

```
console(config)#spanning-tree mst 1 priority 4096
```

**spanning-tree portfast**

Use the `spanning-tree portfast` command in Interface Configuration mode to enable portfast mode. In portfast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable portfast mode, use the `no` form of this command.

**Syntax**

- `spanning-tree portfast`
- `no spanning-tree portfast`

**Default Configuration**

Portfast mode is disabled.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command only applies to access ports. The command is to be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

An interface with portfast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting the standard forward-time delay.
Example

The following example enables portfast on Gi1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)#spanning-tree portfast
```

spanning-tree portfast bpdudfilter default

The `spanning-tree portfast bpdudfilter default` command disables the transmission and reception of BPDUs on portfast enabled ports. Use the “no” form of the command to enable the transmission and receipt of BPDUs.

Syntax

```
spanning-tree portfast bpdudfilter default
no spanning-tree portfast bpdudfilter default
```

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration mode, Interface Configuration mode (physical interface and port-channels)

User Guidelines

BPDU filtering disables both the sending and receiving of BPDUs on portfast enabled ports.

A port enabled for BPDU filtering does not receive or send any BPDUs. It is possible that a network loop may result if BPDU filtering is enabled on a port connected to anything other than an end system.

BPDU filtering is appropriate for configuration on portfast enabled interfaces that are connected to end system hosts where it is desired to not send BPDUs to the host or receive BPDUs from the host. Use the BPDU guard capability if it is desired to obtain a greater level of protection from rogue hosts or possible spanning-tree loops.
The administrator must ensure that interfaces enabled for BPDU filtering are configured as edge ports. Use the `spanning-tree portfast` command to configure the interface as an edge port.

**Example**

The following example discards BPDUs received on spanning-tree ports in portfast mode.

```
console(config)#spanning-tree portfast bpdufilter default
```

### spanning-tree portfast default

Use the `spanning-tree portfast default` command to enable portfast mode on access ports. Interfaces configured as access mode ports are considered to be edge ports. Use the `no` form of this command to disable portfast mode on all ports.

**Syntax**

```
spanning-tree portfast default
no spanning-tree portfast default
```

**Default Configuration**

Portfast mode is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command only affects access ports.

**NOTE:** This command should be used with care. An interface with portfast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting for the standard forward-time delay. Setting a port connected to another switch into portfast mode may cause an accidental topology loop and disrupt switch and network operations.
Example
The following example enables portfast mode on all access ports.

```
console(config)#spanning-tree portfast default
```

**spanning-tree port-priority (Interface Configuration)**

Use the `spanning-tree` port-priority command in Interface Configuration mode to configure the priority value of an edge-port or point-to-point interface to allow the operator to select the relative importance of the interface in the selection process for forwarding. Set this value to a lower number to prefer an operationally enabled interface for forwarding of frames. Use the `no` form of the command to return the priority to the default value.

**Syntax**

```
spanning-tree [vlan vlan-id] port-priority priority
no spanning-tree [vlan vlan-id] port-priority
```

- `vlan-id` — An optional parameter specifying the VLAN to which the priority applies when the port is configured as an edge-port. Range 1-4093.
- `priority` — The priority of the edge-port or point-to-point link in the forwarding port selection process. Range is 0 to 240 in increments of 16.

**Default Configuration**

The default port-priority for IEEE STP is 128.

**Command Mode**

Interface Configuration mode

**User Guidelines**

If the VLAN parameter is given, the priority is configured only for the selected VLANs (applies only when pvst or rapid-pvst mode is selected). Configuration without the VLAN parameter configures the port priority for RSTP, STP-PV, and RSTP-PV.
If an interface is configured with both the `spanning-tree vlan vlan-id port-priority priority` command and the `spanning-tree port-priority priority` command, the `spanning-tree vlan vlan-id port-priority priority` value is used as the port priority.

If a VLAN parameter is provided, the VLAN must have been previously configured or an error is thrown.

An edge port is a port with spanning-tree port-fast enabled. A point-to-point link is a link configured as full-duplex. Edge-ports and point-to-point links directly transition to the forwarding state and do not delay for the listening and learning stages of spanning-tree. An edge port that receives a BPDU is no longer considered an edge-port and will utilize the configured port priority value.

All interfaces and VLANs have 128 as priority value by default. By default, spanning-tree puts the lowest numbered operationally enabled interface in the forwarding state and blocks other interfaces. The priority value is used to override this default behavior. Interfaces with lower port priorities are preferred for forwarding over interfaces with numerically higher priority values. STP-PV/RSTP-PV uses the port priority value when the LAN port is configured as an edge port and uses the VLAN priority value when the interface is configured as a point-to-point link. MSTP uses the port priority regardless of whether the port is an edge port or not.

**Example**

The following example configures a port connected to a host to be least likely to be selected for forwarding to the root bridge, even if the host begins to send BPDUs.

```
console(config-if-Gi1/0/1)#spanning-tree port-priority 240
console(config-if-Gi1/0/1)#spanning-tree vlan 10 port-priority 240
```

**spanning-tree priority**

Use the `spanning-tree priority` command in Global Configuration mode to configure the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning-tree priority use the `no` form of this command.
**Syntax**

spanning-tree priority priority
no spanning-tree priority

- priority — Priority of the bridge. (Range: 0–61440)

**Default Configuration**
The default bridge priority for IEEE STP is 32768.

**Command Mode**
Global Configuration mode

**User Guidelines**
The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Bridge priority configuration is given preference over root primary/secondary configuration. Root primary/secondary configuration is given preference over DRC configuration.

**Example**
The following example configures spanning-tree priority to 12288.

```
console(config)#spanning-tree priority 12288
```

**spanning-tree tcnguard**
Use the `spanning-tree tcnguard` command to prevent a port from propagating topology change notifications. Use the “no” form of the command to enable TCN propagation.

**Syntax**

spanning-tree tcnguard
no spanning-tree tcnguard

**Default Configuration**
TCN propagation is disabled by default.
**Command Mode**

Interface Configuration (Ethernet, Port Channel) mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example configures spanning-tree tcnguard on 4/0/1.

console(config-if-4/0/1)#spanning-tree tcnguard

**spanning-tree transmit hold-count**

Use the `spanning-tree transmit hold-count` command to set the maximum number of BPDUs that a bridge is allowed to send within a hello time window (2 seconds). Use the `no` form of this command to reset the hold count to the default value.

**Syntax**

`spanning-tree transmit hold-count <value>`

`no spanning-tree transmit`

- value — The maximum number of BPDUs to send (Range: 1–10).

**Default Configuration**

The default hold count is 6 BPDUs.

**Command Mode**

Global Configuration mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example sets the maximum number of BPDUs sent to 6.

console(config)#spanning-tree transmit hold-count 6
spanning-tree uplinkfast

Use the spanning-tree uplinkfast command to configure the rate at which gratuitous frames are sent (in packets per second) after a switchover to an alternate port on STP-PV and RSTP-PV configured switches and enable Direct Link Rapid Convergence on STP-PV switches. This command assists in accelerating spanning-tree convergence after switchover to an alternate port.

Use the no form of the command to return the configured rate to the default value (or disable uplinkfast on STP-PV configured switches).

**Syntax**

```
spanning-tree uplinkfast [max-update-rate packets/s ]

no spanning-tree uplinkfast [max-update-rate]
```

- **max-update-rate**—The rate at which update packets are sent. (Range: 0-32000)

**Default Configuration**

The default rate is 150.

**Command Modes**

Global Configuration Mode

**User Guidelines**

DirectLink Rapid Convergence (DRC) can be configured even if the switch is configured for MST(RSTP) mode. It only has an effect when the switch is configured for STP-PV or RSTP-PV modes. Enabling DRC sets the switch priority to 49152. Path costs have an additional 3000 added when DRC is enabled. This reduces the probability that the switch will become the root switch.

DRC immediately changes to an alternate root port on detecting a root port failure and change the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), DRC multicasts a gratuitous frame on the new root port on behalf of each attached machine so
that the rest of the network knows to use the secondary link to reach that machine.

DRC is disabled when the administrator modifies the spanning-tree priority of a VLAN and is re-enabled only when the default priority is restored.

Configuration of the bridge priority is given preference over configuration of the root primary or root secondary configuration, which is given preference over the configuration of DirectLink Rapid Convergence.

RSTP-PV embeds support for IRC and DRC. There is no provision to enable or disable these features in RSTP-PV configured switches.

DRC is most useful for enterprise wiring-closet topologies with a limited number of VLANs. Do not enable DRC on backbone or distribution layer switches as DRC is not capable of completing the reconfiguration of large networks within the max age time.

Example

```
console(config)#spanning-tree uplinkfast
```

**spanning-tree vlan**

Use the `spanning-tree vlan` command to enable per VLAN spanning tree on a VLAN. Use the `no` form of the command to remove the VLAN as a separate spanning tree instance.

**Syntax**

```
spanning-tree vlan {vlan-list}
no spanning-tree vlan {vlan-list}
```

- `vlan-list`–A single VLAN ID or a list of VLAN IDs in comma delineated or range format with no embedded blanks. Range 1-4093.

**Default Configuration**

By default, each configured VLAN is automatically associated with a per VLAN spanning tree instance. If more than eight VLANs are configured, the excess VLANs do not participate in per VLAN spanning tree.
To change the allocation of spanning-tree instances to VLANs, use the **no spanning-tree vlan** command to disassociate a VLAN from a per VLAN spanning-tree instance and use the **spanning-tree vlan** command to associate the spanning-tree instance with the desired VLAN.

**Command Modes**
Global Configuration mode

**User Guidelines**
This command can be configured even if the switch is configured for MST(RSTP) mode. It is only used when the switch is configured for STP-PV or RSTP-PV modes.

**Example**
This example configures a switch to use per VLAN spanning tree for VLANS 12, 13 and 24-26

```
console(config)#spanning-tree vlan 12,13,24-26
```

**spanning-tree vlan forward-time**

Use the **spanning-tree vlan forward-time** command to configure the spanning tree forward delay time for a specified VLAN or a range of VLANs. Use the **no** form of the command to return the forward time to its default value.

**Syntax**

```
spanning-tree vlan vlan-list forward-time 4-30
no spanning-tree vlan vlan-list forward-time
```

- forward-time — The interval (time spent in listening and learning states) before transitioning a port to the forwarding state. (Range: 4-30 seconds)

**Default Configuration**
The default forward delay time is 15.
Command Modes
Global Configuration Mode

User Guidelines
Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end to end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay and the message age overestimate values specific to their network when configuring this parameter.

Forward delay is only application to STP modes. The forward delay setting is ignored in MSTP, RSTP and RSTP-PV modes as the designated port is transitioned to the forwarding state immediately.

Example
console(config)#spanning-tree vlan 3 forward-time 12

spanning-tree vlan hello-time
Use the spanning-tree vlan hello-time command to configure the spanning tree hello time for a specified VLAN or a range of VLANs.

Syntax
spanning-tree vlan vlan-list hello-time 1-10
no spanning-tree vlan vlan-list hello-time
  • Hello-time–The interval between sending successive BDPUs. Default: 2 seconds.

Default Configuration
The default hello time is 2 seconds.

Command Modes
Global Configuration Mode
**User Guidelines**

This command can be configured even if the switch is configured for MST(RSTP) mode. It is only used when the switch is configured for STP-PV or RSTP-PV modes.

Set this value to a lower number to accelerate discovery of topology changes. Use the **no** form of the command to return the hello time to its default value.

**Example**

```bash
console(config)#spanning-tree vlan 3 hello-time 1
```

**spanning-tree vlan max-age**

Use the `spanning-tree vlan max-age` command to configure the spanning tree maximum age time for a set of VLANs. Use the **no** form of the command to return the maximum age timer to the default value.

**Syntax**

```
spanning-tree vlan vlan-list max-age 6-40
no spanning-tree vlan vlan-list > max-age
```

- **max-age** — The maximum age time before a bridge port saves its configuration information.

**Default Configuration**

The default maximum aging time is 20 seconds.

**Command Modes**

Global Configuration Mode

**User Guidelines**

Set this value to a lower number to accelerate discovery of topology changes. The network operator must take into account the end to end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.
The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values. IEEE 802.1Q notes that RSTP and MSTP treat the common spanning tree message age field as a hop count. Section 13.37 Performance discusses appropriate and recommended values and further refers the network operator to the discussion in IEEE 802.1D section 17.14. In particular, operators should make themselves of the requirement that bridges must enforce the following constraint:

\[ 2 \times (\text{Bridge Forward Delay} - 1.0 \text{ seconds}) \geq \text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ seconds}) \]

**Example**

```
console(config)#spanning-tree vlan 3 max-age 18
```

**spanning-tree vlan root**

Use the **spanning-tree vlan root primary** command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value to a lower value calculated to ensure the bridge is the root (or standby) bridge. Use the **no** form of the command to let the network elect the root bridge.

**Syntax**

```
spanning-tree vlan vlan-list root {primary | secondary}
no spanning tree vlan vlan-list root
```

**Default Configuration**

The default bridge priority value is 32768.

**Command Modes**

Global Configuration mode
**User Guidelines**

This command can be configured even if the switch is configured for MST (RSTP) mode. It is only used when the switch is configured for STP-PV or RSTP-PV modes.

The logic sets the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs. This command only applies when STP-PV or RSTP-PV is enabled. Configuration of the bridge priority is given preference over configuration of the root primary or root secondary configuration, which is given preference over the configuration of DirectLink Rapid Convergence.

**Example**

```
case(config)#spanning-tree vlan 3 root primary
```

**spanning-tree vlan priority**

Use the `spanning-tree vlan priority` command to configure the bridge priority of a VLAN. The bridge priority is combined with the MAC address of the switch and is used to select the root bridge for the VLAN. Use the `no` form of the command to return the priority to the default value.

**Syntax**

```
spanning-tree vlan {vlan-list} priority priority
no spanning-tree vlan {vlan-list} priority
```

- **vlan-list**—A single VLAN ID or a list of VLAN IDs in comma delineated or range format with no embedded blanks. Range 1-4093.
- **priority**—The bridge priority advertised when combined with the switch MAC address. Range 0-61440.

**Default Configuration**

The default bridge priority is 32768.

Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.
If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

**Command Modes**

Global Configuration mode

**User Guidelines**

This command can be configured even if the switch is configured for MST(RSTP) mode. It is only used when the switch is configured for STP-PV or RSTP-PV modes.

The root bridge for a VLAN should be carefully selected to provide optimal paths for traffic through the network. Generally, this means selecting a switch that is well-connected with other switches in the network.

Configuration of the bridge priority is given preference over configuration of the root primary or root secondary configuration, which is given preference over the configuration of DirectLink Rapid Convergence.

**Example**

This example configures a switch to be the spanning tree root bridge for VLANs 12, 13, 24, 25, and 26. This presumes other switches in the network utilize the default bridge priority configuration.

```
console(config)#spanning-tree vlan 12,13,24-26 priority 8192
```
UDLD Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The UDLD feature detects unidirectional links on physical ports. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction. UDLD must be enabled on the both sides of the link in order to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

UDLD enabled devices send announcements to the multicast destination address 01-00-0c-cc-cc-cc. UDLD packets are transmitted using SNAP encapsulation, with OUI value 0x00000c (Cisco) and protocol ID 0x0111.

UDLD is supported on individual physical ports that are members of port channel interface. If any of the aggregated links becomes unidirectional, UDLD detects it and disables the individual link, but not the entire port channel. This improves fault tolerance of port-channel.

UDLD PDUs act as network control packets. They are unaffected by Spanning Tree state. Thus, they are transmitted and received regardless of Spanning Tree state.

For the successful operation of UDLD, it is required that its neighbors are UDLD-capable and UDLD is enabled on the corresponding ports. All ports should also be configured to use the same mode of UDLD, either normal or aggressive mode.

Detecting Unidirectional Links on a Device Port

A device detects unidirectional links on its port via UDLD. Every UDLD-capable device distributes service information over the network via a layer 2 broadcast frame. This service frame contains information about sender (source device) and all discovered neighbors. Every sender expects to receive an UDLD echo frame. If an echo frame is received, but does not contain information about the sender itself, it implies that the sender's frames have not reached the neighbors. This can happen when the link is able to receive traffic but cannot send traffic. In other words, a UDLD-capable device can
recognize only the sending failures on unidirectional links. If all devices in the network support UDLD, this functionality is enough to detect all unidirectional links.

**Processing UDLD Traffic from Neighbors**

Every UDLD-capable device collects information about all other UDLD-capable devices. Each device populates UDLD echo packets with collected neighbor information to help neighbors identify unidirectional links. Every frame basically contains the device ID of the sender and the collection of device IDs of its discovered neighbors.

**UDLD in Normal-mode**

In normal mode, a port’s state is classified as **undetermined** if an anomaly exists. These include the absence of its own information in received UDLD messages or the failure to receive UDLD messages. The state of **undetermined** has no effect on the operation of the port. The port is not disabled and continues operating as it previously did. When in normal mode, a port is diagnostically disabled for the following cases:

a. UDLD PDU is received from partner that does not have the port’s own details (echo).

b. When there is a loopback, information sent out on a port is received back as is.

**UDLD in Aggressive-mode**

Aggressive mode differs from normal UDLD mode – it can diagnostically disable a port if the port does not receive any UDLD echo packets after a bidirectional connection was established. It expands the cases when port can be disabled. There can be several causes for a port not to receive UDLD echoes. These include:

- A link is up on one side and down on the other. This can occur on fiber ports if the transmit port is unplugged on one side.
- Loss of connectivity, i.e. the port is neither transmitting nor receiving, but the port also reports it is up.
UDLD will put the port into the diagnostically disabled state in the following cases:

- **a** When there is a loopback, the device ID and port ID sent out on a port is received back.
- **b** UDLD PDU is received from a partner does not have its own details (echo).
- **c** Bidirectional connection is established and no UDLD packets are received from the partner device within three times the message interval.
- **d** In aggressive mode, when the partner does not respond to an ECHO within 7 seconds.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>udld enable (Global Configuration)</td>
</tr>
<tr>
<td>udld reset</td>
</tr>
<tr>
<td>udld message time</td>
</tr>
<tr>
<td>udld timeout interval</td>
</tr>
<tr>
<td>udld enable (Interface Configuration)</td>
</tr>
<tr>
<td>udld port</td>
</tr>
<tr>
<td>show udld</td>
</tr>
</tbody>
</table>

**udld enable (Global Configuration)**

Use the `udld enable` command in Global Configuration mode to globally enable UDLD.

Use the `no` form of the command to globally disable UDLD.

**Syntax**

- `udld enable`
- `no udld enable`

**Default Configuration**

UDLD is disabled by default.
**Command Mode**
Global Configuration mode

**User Guidelines**
This command globally enables UDLD. Interfaces must also be individually enabled for UDLD.

**Example**
This command globally enables UDLD.
```
console(config)#udld enable
```

**udld reset**
Use the `udld reset` command to reset (enable) all interfaces disabled by UDLD.

**Syntax**
```
udld reset
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
The following commands will reset an interface disabled by UDLD:
- Use `udld reset` to reset all interfaces disabled by UDLD.
- The shutdown command followed by no shutdown interface configuration command.
- The no udld enable global configuration command followed by the udld enable command.
- The no udld port interface configuration command followed by the udld port or udld port aggressive interface configuration command.
Example
This example resets all UDLD disabled interfaces.

console#udld reset

udld message time

Use the udld message time command in Global Configuration mode to configure the interval between the transmission of UDLD probe messages on ports that are in the advertisement phase.

Use the no form of the command to return the message transmission interval to the default value.

Syntax
udld message time message-interval

no udld message time

- message-interval—UDLD message transmit interval in seconds. Range is 7 to 90 seconds.

Default Configuration
The default message transmit interval is 15 seconds.

Command Mode
Global Configuration mode

User Guidelines
Lower message time values will detect the unidirectional links more quickly at the cost of higher CPU utilization.

The message interval is also used to age out UDLD entries from the internal database. UDLD entries are removed after three times the message interval and the discovery process starts again.

Example
This example sets the UDLD message transmit interval to 10 seconds.

console(config)#udld message time 10
**udld timeout interval**

Use the `udld timeout interval` command in Global Configuration mode to configure the interval for the receipt of ECHO replies. Use the `no` form of the command to return the value to the default setting.

**Syntax**

```
uudld timeout interval timeout-interval
no udld timeout interval
```

- `timeout-interval`—UDLD timeout interval. Range is 5 to 60 seconds.

**Default Configuration**

The default timeout interval is 5 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command sets the time interval used to determine if the link has bidirectional or unidirectional connectivity. If no ECHO replies are received within three times the message interval, then the link is considered to have unidirectional connectivity.

**Example**

This example sets the UDLD timeout interval to 15 seconds.

```
console(config)#udld timeout interval 15
```

**udld enable (Interface Configuration)**

Use the `udld enable` command in Interface (physical) Configuration mode to enable UDLD on a specific interface. Use the `no` form of the command to disable UDLD on an interface.

**Syntax**

```
udld enable
```
no udld enable

Default Configuration
UDLD is disabled by default on an interface. UDLD must be enabled globally and on an interface in order to operate.

Command Mode
Interface (physical) Configuration mode

User Guidelines
UDLD cannot be enabled on a port channel. Instead, enable UDLD on the physical interfaces of a port channel.

Example
This example enables UDLD on an interface. UDLD must also be enabled globally.

console(config-if-Tel/0/1)#udld enable

udld port
Use the udld port command in Interface (physical) Configuration mode to select the UDLD operating mode on a specific interface.
Use the no form of the command to reset the operating mode to the default (normal).

Syntax
udld port aggressive
no udld port

• aggressive—Sets the port to discover peers in aggressive mode.

Default Configuration
Normal mode is configured by default when UDLD is enabled on an interface.
**Command Mode**
Interface (Ethernet) Configuration mode

**User Guidelines**
In aggressive mode, UDLD will attempt to detect a peer by sending an ECHO packet every seven seconds until a peer is detected.

**Example**
This example configure an interface to operate in UDLD aggressive mode.
```
console(config-if-Te1/0/1)#udld port aggressive
```

**show udld**
Use the `show udld` command in User Exec or Privileged Exec mode to display the global settings for UDLD.

**Syntax**
```
show udld [interface-id|all]
```

**Default Configuration**
This command has no default setting.

**Command Mode**
Privileged Exec or User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
When no interface is specified, the following fields are shown:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>The global administrative mode of UDLD.</td>
</tr>
<tr>
<td>Message Interval</td>
<td>The time period (in seconds) between the transmission of UDLD probe packets.</td>
</tr>
</tbody>
</table>
When an interface ID is specified, the following fields are shown:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Id</td>
<td>The interface identifier in short form, e.g. te1/0/1.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>The administrative mode of UDLD configured on this interface. This is either Enabled or Disabled.</td>
</tr>
<tr>
<td>UDLD Mode</td>
<td>The UDLD mode configured on this interface. This is either Normal or Aggressive.</td>
</tr>
<tr>
<td>UDLD Status</td>
<td>The status of the link as determined by UDLD. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Undetermined – UDLD has not collected enough information to determine the state of the port.</td>
</tr>
<tr>
<td></td>
<td>• Not applicable – UDLD is disabled, either globally or on the port.</td>
</tr>
<tr>
<td></td>
<td>• Shutdown – UDLD has detected a unidirectional link and shutdown the port. That is, the port is in the D-Disable state.</td>
</tr>
<tr>
<td></td>
<td>• Bidirectional - UDLD has detected a bidirectional link.</td>
</tr>
<tr>
<td></td>
<td>• Undetermined (Link Down) – The port transitions into this state when the port link physically goes down due to any reasons other than the port being put into D-Disable mode by the UDLD protocol on the switch.</td>
</tr>
</tbody>
</table>

**Command History**

Modified in version 6.5 firmware.

**Example**

The output of the `show udld all` command must (at least) show the err-disable status for UDLD err-disabled interfaces and shutdown for the administratively disabled interfaces.

console#show udld all
<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>UDLD Mode</th>
<th>UDLD Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>Aggressive</td>
<td>Err-disabled (Link Down)</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>Aggressive</td>
<td>UDLD Err-disabled</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enabled</td>
<td>Aggressive</td>
<td>Shutdown (Link Down)</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Disabled</td>
<td>Normal</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Disabled</td>
<td>Normal</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
VLAN Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dell EMC Networking 802.1Q VLANs are an implementation of the Virtual Local Area Network, specification 802.1Q. Operating at Layer 2 of the OSI model, the VLAN is a means of parsing a single network into logical user groups or organizations as if they physically resided on a dedicated LAN segment of their own. In reality, this virtually defined community may have individual members scattered across a large, extended LAN. The VLAN identifier is part of the 802.1Q tag, which is added to an Ethernet frame by an Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first three bits of the 802.1Q tag are used by 802.1p to establish priority for the packet.

Dell EMC Networking switches supports 802.1Q VLANs. As such, ports may simultaneously belong to multiple VLANs. VLANs allow a network to be logically segmented without regard to the physical locations of devices in the network.

Dell EMC Networking switches supports up to 4093 VLANs for forwarding. Interfaces can be configured in trunk mode (multiple VLAN support) or access mode (single VLAN support).

VLANs can be allocated by subnet and netmask pairs, thus allowing overlapping subnets. For example, subnet 10.10.128.0 with Mask 255.255.128.0 and subnet 10.10.0.0 with Mask 255.255.0.0 can have different VLAN associations.

Access, trunk and general mode VLAN configurations are maintained independently by the switch and take affect when the interface is configured in the relevant mode. In other words, trunk mode VLAN configuration only affects an interface when it is configured in trunk mode. When the interface is configured in trunk mode, access and general mode VLAN configuration is ignored.
Double VLAN Mode

An incoming frame is identified as tagged or untagged based on Tag Protocol Identifier (TPID) value it contains. The IEEE 802.1Q standard specifies a TPID value (0x8100) to recognize an incoming frame as tagged or untagged. Any valid Ethernet frame with a value of 0x8100 in the 12th and 13th bytes is recognized as a tagged frame.

Dell EMC Networking N-Series switches can be configured to enable the port in double-VLAN (QinQ) mode. In this mode, the switch looks for 12th, 13th, 16th, and 17th bytes for the tag status in the incoming frame. The outer tag TPID is identified by the 12th and 13th bytes values. The inner tag TPID is identified by 16th and 17th bytes values. These two TPID values can be different or the same. VLAN normalization, source MAC learning, and forwarding are based on the outer value in a received frame.

Independent VLAN Learning

Independent VLAN Learning (IVL) allows unicast address-to-port mappings to be created based on a MAC Address in conjunction with a VLAN ID.

This arrangement associates the MAC Address only with the VLAN on which the frame was received. Therefore, frames are forwarded based on their unicast destination address as well as their VLAN membership. This configuration affords multiple occurrences of an address in the forwarding database. Each address associates with a unique VLAN. Care must be taken in the administration of networks, as multiple instances of a MAC address, each on a different VLAN, can quickly eat up address entries.

Each VLAN is associated with its own forwarding database. Hence the number of forwarding databases equals the number of VLANs supported. The MAC address stored is supplemented by a 2-byte VLAN ID. The first 2 bytes of a forwarding database entry contain the VLAN ID associated, and the next 6 bytes contain the MAC address. There is a one-to-one relationship between VLAN ID and FID (forwarding database ID).
Protocol Based VLANs

The main purpose of Protocol-based VLANs (PBVLANs) is to selectively process packets based on their upper-layer protocol by setting up protocol-based filters. Packets are bridged through user-specified ports based on their protocol.

In PBVLANs, the VLAN classification of a packet is based on its protocol (IP, IPX, NetBIOS, and so on). PBVLANs help optimize network traffic because protocol-specific broadcast messages are sent only to end stations using that protocol. End stations do not receive unnecessary traffic, and bandwidth is used more efficiently. It is a flexible method that provides a logical grouping of users. An IP subnet or an IPX network, for example, can each be assigned its own VLAN. Additionally, protocol-based classification allows an administrator to assign nonrouting protocols, such as NetBIOS or DECnet, to larger VLANs than routing protocols like IPX or IP. This maximizes the efficiency gains that are possible with VLANs.

In port-based VLAN classification, the Port VLAN Identifier (PVID) is associated with the physical ports. The VLAN ID (VID) for an untagged packet is equal to the PVID of the port. In port-and protocol-based VLAN classifications, multiple VIDs are associated with each of the physical ports. Each VID is also associated with a protocol. The ingress rules used to classify incoming packets include the use of the packet's protocol, in addition to the PVID, to determine the VLAN to which the packet belongs. This approach requires one VID on each port for each protocol for which the filter is desired.

IP Subnet Based VLANs

This feature allows an untagged packet to be placed in a configured VLAN based upon its IP address.

MAC-Based VLANs

This feature allows an untagged packet to be placed in a configured VLAN based upon its MAC address.
Private VLAN Commands

The Dell EMC Networking Private VLAN feature separates a regular VLAN domain into two or more subdomains. Each subdomain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all subdomains that belong to a private VLAN. The secondary VLAN ID differentiates subdomains from each another and provides Layer 2 isolation between ports of the same private VLAN. There are the following types of VLANs within a private VLAN:

- Primary VLAN
  Forwards the traffic from the promiscuous ports to isolated ports, community ports and other promiscuous ports in the same private VLAN. Only one primary VLAN can be configured per private VLAN. All ports within a private VLAN share the same primary VLAN.

- Isolated VLAN
  Is a secondary VLAN. It carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.

- Community VLAN
  Is a secondary VLAN. It forwards traffic between ports which belong to the same community and to the promiscuous ports. There can be multiple community VLANs per private VLAN.

Three types of port designations exist within a private VLAN:

- Promiscuous port
  Belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports and isolated ports. An endpoint connected to a promiscuous port is allowed to communicate with any endpoint within the private VLAN. Multiple promiscuous ports can be defined for a single private VLAN domain.

- Host port
  Belongs to a secondary VLAN and depending upon the type of secondary VLAN can either communicate with other ports in the same community (if the secondary VLAN is the community VLAN) and with the
promiscuous ports or can communicate only with the promiscuous ports (if the secondary VLAN is an isolated VLAN).

The Private VLANs can be extended across multiple switches through inter-switch/stack links that transport primary, community and isolated VLANs between devices, as shown in Figure 3-1.

**Figure 3-1. Private VLANs**

![Private VLAN Diagram]

**Isolated VLAN**

An endpoint connected over an isolated VLAN is allowed to communicate with endpoints connected to promiscuous ports only. Endpoints connected to adjacent endpoints over an isolated VLAN cannot communicate with each other.

**Community VLAN**

An endpoint connected over a community VLAN is allowed to communicate with the endpoints within the community and can also communicate with any configured promiscuous port. The endpoints which belong to one community cannot communicate with endpoints which belong to a different community or with endpoints connected over isolated VLANs.
Private VLAN Operation in the Switch Environment

The Private VLAN feature operates in a stacked or single switch environment. The stack links are transparent to the configured VLAN, thus there is no need for special private VLAN configuration. Any private VLAN port can reside on any stack member.

In order to enable Private VLAN operation across multiple switches which are not stacked, the inter-switch links should carry VLANs which belong to a private VLAN. The trunk ports which connect neighbor switches have to be assigned to the primary, isolated, and community VLANs of a private VLAN.

In regular VLANs, ports in the same VLAN switch traffic at L2. However for private VLAN, the promiscuous port is in the primary VLAN whereas the isolated or community ports are in the secondary VLAN. Similarly, for broadcasts, in regular VLANs, ports in the same VLAN receive broadcast traffic. However, for private VLANs, the ports to which the broadcast traffic is forwarded depend on the type of port on which the traffic was received. If the received port is a host port; the traffic is forwarded to all promiscuous and trunk ports. If the received port is community port the broadcast traffic is forwarded to promiscuous, trunk and community ports in the same VLAN. A promiscuous port sends traffic to other promiscuous ports, isolated and community ports.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan show port protocol</td>
<td>switchport general acceptable-frame-type tagged-only</td>
</tr>
<tr>
<td>interface range vlan show switchport ethertype</td>
<td>switchport trunk encapsulation dot1q</td>
</tr>
<tr>
<td>name (VLAN Configuration) show vlan</td>
<td>switchport general allowed vlan</td>
</tr>
<tr>
<td>private-vlan show vlan association mac</td>
<td>switchport general ingress-filtering disable</td>
</tr>
<tr>
<td></td>
<td>switchport general pvid</td>
</tr>
<tr>
<td></td>
<td>vlan association mac</td>
</tr>
<tr>
<td></td>
<td>vlan association subnet</td>
</tr>
</tbody>
</table>
interface vlan

Use the `interface vlan` command in Global Configuration mode to enable L3 on a VLAN and enter VLAN Interface Configuration mode. Use the `no` form of the command to disable routing on the VLAN.

**Syntax**

```plaintext
interface vlan {vlan-id}
no interface vlan { vlan-id }
```

- `vlan-id`—The ID of a valid VLAN (Range 1–4093).

**Default Configuration**

By default, Layer 3 is enabled on VLAN 1 on the N1100-ON/N1500/N2000/N2100-ON Series switches. However, VLAN routing interfaces do not route packets until an IP address is assigned to the VLAN and IP routing is globally enabled. DHCP and Layer 3 are not enabled on VLAN 1 by default for the N3000, N3100-ON, and N4000 Series switches. DHCP is enabled on VLAN 1 by default for the N1100-ON/N1500/N2000/N2100-ON switches. The N1100-ON does not support routing.

**Command Mode**

VLAN Configuration or Global Configuration modes
User Guidelines
Assigning an IP address to a VLAN interface enables Layer 3 on the VLAN interface. If IP routing is globally enabled and an IP address is assigned, the router will route packets to and from the VLAN. When an interface is enabled for routing using the `interface vlan` command, the port will no longer be operationally enabled as a protected port on the interface.

Use the `no` form of the command to remove empty interface vlan entries from the running config.

Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the L3 address of the switch. Packets received over the configured VLAN which are addressed to the L3 address are processed by the switch CPU. This includes SNMP/HTTP/Telnet/SNMP and any other configured management protocols. If a subsequent VLAN is configured with an IP address, the prior VLAN configuration is removed. Dell EMC N1100-ON switches do not support routing.

When an interface is enabled for routing, the port will no longer be operationally enabled as a protected port on the interface. Routing cannot be operationally enabled on a port that is a member of a port-channel or a port mirroring probe port.

Examples
```
console(config-vlan10)# interface vlan 10
console(config-if-vlan10)#
```

interface range vlan

Use the `interface range vlan` command in Global Configuration mode to enable routing on a range of VLANs and to execute a command on multiple VLANs at the same time.

Syntax
```
interface range vlan {vlan-id | all}
```

- `vlan-id` — A list of valid VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1–4093)
- `all` — All existing static VLANs.
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
The VLANs in the interface range must be configured and enabled for routing prior to use in the `vlan range` command. Commands used in the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

Example
The following example groups VLAN 221 through 228 and VLAN 889 to execute the commands entered in interface range mode.

```
dellswitch(config)#vlan 2-5
dellswitch(config-vlan2-5)#exit
dellswitch(config)#interface vlan 2
dellswitch(config-if-vlan2)#interface vlan 3
dellswitch(config-if-vlan3)#interface vlan 4
dellswitch(config-if-vlan4)#interface vlan 5
dellswitch(config-if-vlan5)#interface range vlan 2-5
dellswitch(config-if)#
```

name (VLAN Configuration)
Use the `name` command in VLAN Configuration mode to configure the VLAN name. To return to the default configuration, use the `no` form of this command.

NOTE: This command cannot be configured for a range of interfaces (range context).

Syntax
```
name vlan–name
no name
```
- `vlan–name`—The name of the VLAN. Must be 1–32 characters in length.
Default Configuration
The default VLAN name is default.

Command Mode
VLAN Configuration mode

User Guidelines
The VLAN name may include any alphanumeric characters including a space, underscore, or dash. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may truncate entries at the first illegal character or reject the entry entirely. The name of VLAN 1 cannot be changed.

Example
The following example configures a VLAN name of office2 for VLAN 2.

```
console(config)#vlan 2
console(config-vlan2)#name “RDU-NOC Management VLAN”
```

private-vlan
Use the private-vlan command in VLAN Configuration mode to define a private VLAN association between the primary and secondary VLANs. Use the no form of the command to remove the private VLAN association.

Syntax
private-vlan {primary|isolated|community|association [add|remove] vlan-list}

no private-vlan [association]

- association—Defines an association between the primary VLAN and secondary VLANs.
- primary—Specify that the selected VLAN is the primary VLAN.
- community—Specify that the selected VLAN is the community VLAN.
- isolated—Specify that the selected VLAN is the isolated VLAN.
- add—Associates a secondary VLAN with the primary VLAN.
• **remove**—Deletes the secondary VLAN association with the primary VLAN.

• **vlan-list**—A list of secondary VLAN ids to be mapped to a primary VLAN. The VLAN list can contain multiple entries separated by commas and containing no spaces. Each entry can be a single VLAN id or a hyphenated range of VLANs.

**Default Configuration**

This command has no default setting.

**Command Mode**

VLAN Configuration mode

**User Guidelines**

A community VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

An isolated VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or other isolated ports with the same primary VLAN.

The primary VLAN is the VLAN that carries traffic from a promiscuous port to the private ports.

VLAN 1 cannot be configured in a private VLAN configuration.

**Examples**

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)# private-vlan primary
console(config-vlan)# exit
console(config)# vlan 1001
console(config-vlan)# private-vlan isolated
console(config-vlan)# exit
console(config)# vlan 1002
console(config-vlan)# private-vlan community
console(config-vlan)# exit
console(config)# vlan 1003
console(config-vlan)# private-vlan community
console(config-vlan)# exit
```
protocol group

Use the protocol group command in VLAN Configuration mode to attach a VLAN ID to the protocol-based group identified by groupid. A group may only be associated with one VLAN at a time. However, the VLAN association can be changed. The referenced VLAN should be created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To detach the VLAN from this protocol-based group identified by this groupid, use the no form of this command.

Syntax

protocol group group-id vlan-id

no protocol group group-id vlan-id

- group-id — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the vlan protocol group command. To see the group ID associated with the name of a protocol group, use the show port protocol all command.

- vlan-id — A valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to attach the VLAN ID “100” to the protocol-based VLAN group “3.”

```console
console(config)# vlan 20
console(config-vlan)# private-vlan association 1001-1003
console(config-vlan)# end
```
protocol vlan group

Use the `protocol vlan group` command in Interface Configuration mode to add the physical unit/slot/port interface to the protocol-based group identified by groupid. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove the interface from this protocol-based VLAN group that is identified by this groupid, use the `no` form of this command.

If you select `all`, all ports are removed from this protocol group.

**Syntax**

```
protocol vlan group group-id
no protocol vlan group group-id
```

- **group-id** — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the `vlan protocol group` command. To see the group ID associated with the name of a protocol group, use the `show port protocol all` command.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

This command has no user guidelines.
Example
The following example displays how to add an Ethernet interface to the group ID of “2.”

`console(config-if-Gi1/0/1)#protocol vlan group 2`

**protocol vlan group all**

Use the `protocol vlan group all` command in Global Configuration mode to add all physical interfaces to the protocol-based group identified by groupid. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove all interfaces from this protocol-based group that is identified by this groupid, use the `no` form of the command

**Syntax**

```
protocol vlan group all group-id
no protocol vlan group all group-id
```

- **group-id** — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the `vlan protocol group` command. To see the group ID associated with the name of a protocol group, use the `show port protocol all` command.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example displays how to add all physical interfaces to the protocol-based group identified by group ID “2.”

```
console(config)#protocol vlan group all 2
```

**show dot1q-tunnel**
Use the `show dot1q-tunnel` command to display the QinQ status for each interface.

**Syntax**

```
show dot1q-tunnel [ interface interface-id ]
```

**Default Configuration**
If no interfaces are specified, information is shown for all interfaces.

**Command Mode**
Privileged Exec mode and all show modes

**User Guidelines**
Up to three additional TPIDs can be configured. The 802.1Q tag is pre-defined in the system and cannot be removed.

It is not possible to configure an inner TPID value other than 0x8100.

The primary TPID is shown in the EtherType column. The primary TPID is placed in the outer tag for traffic egressing the interface. The interface will process incoming traffic as double tagged if any of the configured TPIDs is present in the frames outer VLAN tag. Traffic with a TPID other than the configured TPID is processed normally, i.e. as if it is not double tagged.

**Example**
```
console(config)#show dot1q-tunnel interface all
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>EtherType</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Disable</td>
<td>802.1</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Disable</td>
<td>802.1</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Disable</td>
<td>802.1</td>
</tr>
</tbody>
</table>
show interfaces switchport

Use the show interfaces switchport command to display the complete switchport VLAN configuration for all possible switch mode configurations: access, dot1q-tunnel, general, trunk, and (private VLAN) host or (private VLAN) promiscuous.

Syntax

```plaintext
show interfaces switchport {{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}}
```

Default Configuration

If no interface parameter is given, all interfaces are shown.

Command Mode

Privileged Exec mode, Interface Configuration mode and all Configuration submodes

User Guidelines

Each of the switchport modes can be configured independently for a port or port channel. The configurations are retained even when the port is configured in a different mode.

It is recommended that the private VLAN host ports be configured as spanning-tree portfast.

Examples

The following example displays switchport configuration individually for gi1/0/1.

```
switch-top(config-if-Gi1/0/1)#show interfaces switchport gi1/0/1

Port: Gi1/0/1
```
VLAN Membership Mode: Trunk Mode
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Enabled
General Mode Acceptable Frame Type: Admit All
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN Tagging: Disabled
Trunking Mode VLANs Enabled: 1-99,101-4093
Private VLAN Host Association: none
Private VLAN Mapping:
Private VLAN Operational Bindings:
Default Priority: 0
Protected: Disabled
Forbidden VLANs:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>Out</td>
</tr>
</tbody>
</table>

**show port protocol**

Use the `show port protocol` command to display the Protocol-Based VLAN information for either the entire system or for the indicated group.

**Syntax**

`show port protocol {group-id | all}`

- **group-id** — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the `vlan protocol group` command.
- **all** — Enter `all` to show all interfaces.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
The following example displays the Protocol-Based VLAN information for either the entire system.

```
console#show port protocol all
```

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group ID</th>
<th>Protocol(s)</th>
<th>VLAN</th>
<th>Interface(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>1</td>
<td>IP</td>
<td>1</td>
<td>gi1/0/1</td>
</tr>
</tbody>
</table>

show switchport ethertype
Use the `show switchport ethertype` to display the configured Ethertype for each interface.

Syntax
```
show switchport ethertype [ interface interface-id | all ]
```
- interface-id—A physical interface or port channel.
- all—All interfaces.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode and all Show modes

User Guidelines
Up to three additional TPIDs can be configured. The 802.1Q TPID is pre-configured in the system and may not be removed.
It is not possible to configure an inner VLAN TPID value other than 0x8100.
The primary TPID is shown in the EtherType column. The primary TPID is placed in the outer tag for traffic egressing the interface. The interface will process traffic as double tagged if any of the configured TPIDs is present in the frames outer VLAN tag. Traffic with a TPID other than the configured TPID is processed normally, i.e. as if it is not double tagged.

**Example**

This example shows the various invocations of the command.

```bash
console(config)#show switchport ethertype
Default TPID......................... 802.1
Configured TPIDs........................ vMAN Custom (1010)

console(config)#show switchport ethertype interface gi1/0/1
Interface EtherType Secondary TPIDs
--------- --------- ---------------
Gi1/0/1   802.1

console(config-vlan10)#show switchport ethertype interface all

console(config)#show switchport ethertype interface gi1/0/1
Interface EtherType Secondary TPIDs
--------- --------- ---------------
Gi1/0/1   802.1
Gi1/0/2   802.1     VMAN
Gi1/0/3   802.1
Gi1/0/4   802.1
Gi1/0/5   802.1
```

**show vlan**

Use the `show vlan` command to display detailed information, including interface information and dynamic VLAN type, for a specific VLAN or RSPAN VLAN. The ID is a valid VLAN identification number.

**Syntax**

`show vlan [id vlan-id | name vlan-name]`
• vlan-id—A VLAN identifier
• vlan-name—A valid VLAN name (Range 1-32 characters)

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
• VLAN—The VLAN identifier
• Name—The VLAN name
• Ports—The port membership for the VLAN
• Type—The type of VLAN (default, static, dynamic)

Example
This shows all VLANs and RSPAN VLANs.

console#show vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>Po1-128, Gi1/0/1-48</td>
<td>Default</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>Static</td>
</tr>
</tbody>
</table>

RSPAN Vlan

This example shows information for a specific VLAN ID.

console#show vlan id 10

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td>Tel1/0/1</td>
<td>Static</td>
</tr>
</tbody>
</table>

RSPAN Vlan
This example shows information for a specific VLAN name.

```
show vlan name myspan
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>myspan</td>
<td>Te1/0/1</td>
<td>Static</td>
</tr>
</tbody>
</table>

show vlan association mac

Use the `show vlan association mac` command to display the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

**Syntax**

```
show vlan association mac [mac-address]
```

- `mac-address` — Specifies the MAC address to be entered in the list.
  (Range: Any valid MAC address)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

- MAC Address—The configured MAC address
- VLAN —The associated VLAN identifier
Example
The following example shows no entry in MAC address to VLAN cross-reference.

```
console#show vlan association mac
MAC Address              VLAN ID
-----------------------  -------
0001.0001.0001.0001        1
```

**show vlan association subnet**

Use the `show vlan association subnet` command to display the VLAN associated with a specific configured IP-Address and netmask. If no IP Address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

**Syntax**

```
show vlan association subnet [ip-address ip-mask]
```

- ip-address — Specifies IP address to be shown
- ip-mask — Specifies IP mask to be shown

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

- IP Address—The configured IP address
- IP Mask—The configured IP subnet mask
- VLAN ID—The associated VLAN identifier

**Example**

The following example shows the case if no IP Subnet to VLAN association exists.
console#show vlan association subnet
<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP Mask</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The IP Subnet to VLAN association does not exist.

**show vlan private-vlan**

Use the `show vlan private-vlan` command to display information about the configured private VLANs including primary and secondary VLAN IDs, type (community, isolated, or primary), and the ports which belong to a private VLAN.

**Syntax**

`show vlan private-vlan [type]`

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Do not configure private VLANs on ports configured with any of these features:

- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- Voice VLAN

It is recommended that the private VLAN host ports be configured as spanning-tree portfast.

The command displays the following information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Primary VLAN ID.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Secondary VLAN ID.</td>
</tr>
</tbody>
</table>
switchport access vlan

Use the `switchport access vlan` command in Interface Configuration mode to configure the PVID VLAN ID when the interface is in access mode. To reconfigure the interface to use the default VLAN, use the `no` form of this command.

**Syntax**

```
switchport access vlan vlan-id
no switchport access vlan
```

- `vlan-id` — The identifier of the VLAN associated with the access port.

**Default Configuration**

This command has no default values.

**Command Mode**

Interface Configuration (Ethernet and port channel) mode

**User Guidelines**

This command configures the interface access mode VLAN membership. The `no` form of the command sets the access mode VLAN membership to VLAN 1. It is possible to configure the access mode VLAN identifier when the port is in general or trunk mode. Doing so does not change the VLAN membership of the interface until the interface is configured into access mode.

If the VLAN identified in the command has not been previously created, the system creates the VLAN, issues a message, and associates the VLAN with the interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Secondary VLAN type. Use the <code>type</code> parameter to display only private VLAN ID and its type.</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports that are associated with a private VLAN.</td>
</tr>
</tbody>
</table>

Type Secondary VLAN type. Use the `type` parameter to display only private VLAN ID and its type.

Ports Ports that are associated with a private VLAN.
Examples
The following example configures interface gi1/0/8 to operate in access mode with a VLAN membership of 23. Received untagged packets are processed on VLAN 23. Received packets tagged with VLAN 23 are also accepted. Other received tagged packets are discarded.

```bash
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport access vlan 23
```

The following example sets the PVID for interface Gi1/0/12 to VLAN ID 33. Since VLAN 33 does not exist, it is automatically created.

```bash
console(config)# interface gi1/0/12
console(config-if-Gi1/0/12)# switchport access vlan 33
Access VLAN does not exist. Creating VLAN 33
```

switchport dot1q ethertype (Global Configuration)

Use the `switchport dot1q ethertype` command to define additional QinQ tunneling TPIDs for matching in the outer VLAN tag of received frames. Use the `no` form of the command to remove the configured TPIDs.

**Syntax**

```bash
switchport dot1q ethertype { vman | custom 1-65535 }
no switchport dot1q ethertype { vman | custom 1-65535 }
```

- **vman**—Define the Ethertype as 0x88A8.
- **custom**—Define the Ethertype as a 16 bit user defined value (in decimal).

**Default Configuration**

802.1Q is the default Ethertype for both inner and outer VLAN TPIDs. The 802.1Q TPID cannot be removed from the configuration.

By default QinQ processing of frames is disabled.

**Command Mode**

Global Configuration
User Guidelines

This command globally defines additional TPIDs for use by the system for matching of ingress packets in the outer tag. The switch uses the default primary TPID 0x8100 and any of the additional TPIDs to match packets in the outer tag on ingress. A TPID must be configured globally before it can be applied to an interface. Up to three additional TPIDs can be configured for acceptance in the outer VLAN tag on the SP port. Packets received on the SP port which do not contain one of the configured TPIDs or which do not contain the SP VLAN ID in the outermost VLAN tag are processed by the port as if they are not part of the QinQ tunnel.

Use the no form of the command to remove an additional TPID. Doing so removes the TPID from all interfaces. If the removed TPID is the primary TPID for an interface, the interface is configured to use the default primary TPID 0x8100.

Packets are always transmitted by the system using the primary TPID value in the outer VLAN tag.

It is not possible to configure an inner VLAN TPID value. The inner VLAN TPID value is always 802.1Q (0x8100).

Use the switchport dot1q ethertype Interface Configuration mode command to apply a configured TPID value to an interface.

Example

This example defines the VMAN (0x88A8) TPID for use on a service provider (SP) port and configures a service provider port (Te1/0/1) in general mode after creating the common SP/CE VLAN. The port is configured in general mode and to only allow tagged packets on ingress using the outer VLAN ID 10. Then, the port is configured to accept the VMAN TPID in the outer VLAN on ingress and further configured to tag packets with the VMAN TPID and VLAN ID 10 in the outer VLAN tag on egress.

This example configures an SP port using general mode.

console(config)#switchport dot1q ethertype vman
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport mode general
console(config-if-Te1/0/1)#switchport general allowed vlan add 10 tagged
console(config-if-Te1/0/1)#switchport dot1q ethertype vman primary-tpid
This example configures an SP port using trunk mode.

```
console(config)#switchport dot1q ethertype vman
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport mode trunk
console(config-if-Te1/0/1)#switchport trunk allowed vlan 10
console(config-if-Te1/0/1)#switchport trunk native vlan 10
console(config-if-Te1/0/1)#switchport dot1q ethertype vman primary-tpid
```

### switchport dot1q ethertype (Interface Configuration)

Use the `switchport dot1q ethertype` command to apply previously defined QinQ tunneling TPIDs to a service provider interface. Use the `no` form of the command to remove the configured TPIDs.

**Syntax**

```
switchport dot1q ethertype { 802.1Q | vman | custom 0-65535 } [primary-tpid]
no switchport dot1q ethertype { 802.1Q | vman | custom 0-65535 } [primary-tpid]
```

- **802.1Q**—Allow ingress frames with Ethertype 0x8100.
- **vman**—Define the Ethertype as 0x88A8.
- **custom**—Define the Ethertype as a 16 bit user defined value (in decimal).
- **primary-tpid**—Set the outer VLAN tag TPID to be inserted in frames transmitted on an SP port. Also processes ingress frames with the configured Ethertype as double tagged.

**Default Configuration**

802.1Q is the default Ethertype for both inner and outer VLAN TPIDs. By default QinQ processing of frames is disabled.
**Command Mode**

Interface Configuration mode (physical and port channel), Interface range mode (physical and port channel)

**User Guidelines**

This command applies a previously defined TPID to an interface. The TPID must be configured using the global configuration mode command before it can be applied to an interface. Up to 3 additional TPIDs for use in the outer VLAN tag may be configured.

The outer VLAN tag in tagged packets received on the interface is compared against the configured list of TPIDs. Frames that do not match any of the configured TPIDs are forwarded normally, i.e. without QinQ processing. Frames transmitted on the interface are always transmitted with the primary TPID inserted in the outer VLAN tag.

Use the **no** form of the command to remove the TPID from an interface.

Defining a new primary TPID command overwrites the existing primary TPID for an interface.

The **no** form of the command with the optional primary TPID specified sets the primary TPID value to 802.1Q (0x8100).

If the TPID value was not configured as a primary TPID and the **no** form the command includes the optional **primary-tpid** argument, the command will fail.

If the TPID value was configured as the primary TPID, and the **no** form of the command does not include the optional **primary-tpid** argument, the command will fail.

If a TPID value is configured as the primary TPID, and it is added again without the **primary-tpid** optional argument, the TPID will be treated as the primary TPID (the primary TPID includes the behavior of secondary TPIDs). It is not possible to configure an inner VLAN TPID value. The inner VLAN TPID value is always 802.1Q (0x8100).

**Example**

This example defines the VMAN (0x88A8) TPID for use on a service provider port and configures a service provider port (Te1/0/1) in general mode. The general mode port is configured to only allow tagged packets on ingress using
Layer 2 Switching Commands

VLAN ID 10. Then, in the last command, the port is configured to accept the VMAN TPID in the outer VLAN on ingress and further configured to tag packets with the VMAN TPID in the outer VLAN tag on egress.

```
console(config)#switchport dot1q ethertype vman
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport mode general
console(config-if-Te1/0/1)#switchport general allowed vlan add 10 tagged
console(config-if-Te1/0/1)#switchport dot1q ethertype vman primary-tpid
```

**switchport general forbidden vlan**

Use the `switchport general forbidden vlan` command in Interface Configuration mode to forbid adding specific VLANs to a general mode port. To revert to allowing the addition of specific VLANs to the port, use the `remove` parameter of this command.

**Syntax**

```
switchport general forbidden vlan {add vlan-list | remove vlan-list}
```

- **add vlan-list** — List of valid VLAN IDs to add to the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove vlan-list** — List of valid VLAN IDs to remove from the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

**Default Configuration**

All VLANs allowed.

**Command Mode**

Interface Configuration (Ethernet and port channel) mode
**User Guidelines**

This configuration only applies to ports configured in general mode. It is possible to configure the general mode VLAN membership of a port while the port is in access or trunk mode. Doing so does not change the VLAN membership of the port until it is configured to be in general mode.

**Example**

The following example forbids adding VLAN numbers 234 through 256 to port 1/0/8.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport general forbidden vlan add 234-256
```

`s:witchport general acceptable-frame-type tagged-only`

Use the `switchport general acceptable-frame-type tagged-only` command in Interface Configuration mode to discard untagged frames at ingress. To enable untagged frames at ingress, use the `no` form of this command.

**Syntax**

```
switchport general acceptable-frame-type tagged-only
no switchport general acceptable-frame-type tagged-only
```

**Default Configuration**

All frame types are accepted at ingress.

**Command Mode**

Interface Configuration (Ethernet and port channel) mode

**User Guidelines**

It is possible to configure the general mode acceptable frame types of a port while the port is in access or trunk mode. Doing so does not change the configuration of the port until it is configured to be in general mode.
**Example**
The following example configures 1/0/8 to discard untagged frames at ingress.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport general acceptable-frame-type tagged-only
```

**switchport general allowed vlan**

Use the `switchport general allowed vlan` command in Interface Configuration mode to add VLANs to or remove VLANs from a general port.

**Syntax**

```
switchport general allowed vlan add vlan-list [tagged | untagged]
switchport general allowed vlan remove vlan-list
```

- **add vlan-list** — List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove vlan-list** — List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **tagged** — Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged, the default is untagged.
- **untagged** — Sets the port to transmit untagged packets for the VLANs.

**Default Configuration**
Untagged.

**Command Mode**
Interface Configuration (Ethernet and port channel) mode

**User Guidelines**
Use this command to change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.
It is possible to configure the general mode VLAN membership of a port while the port is in access or trunk mode. Doing so does not change the VLAN membership of the port until it is configured to be in general mode.

**Example**
The following example shows how to add VLANs 1, 2, 5, and 8 to the allowed list.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport general allowed vlan add 1,2,5,8 tagged
```

**switchport general ingress-filtering disable**

Use the `switchport general ingress-filtering disable` command in Interface Configuration mode to disable port ingress filtering. To enable ingress filtering on a port, use the `no` form of this command.

**Syntax**

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

**Default Configuration**

Ingress filtering is enabled.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

Ingress filtering, when enabled, discards received frames that are not tagged with a VLAN for which the port is a member. If ingress filtering is disabled, tagged frames from all VLANs are processed by the switch.

**Example**
The following example shows how to enables port ingress filtering on Gigabit Ethernet interface 1/0/8.


console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport general ingress-filtering enable

**switchport general pvid**

Use the `switchport general pvid` command in Interface Configuration mode to configure the Port VLAN ID (PVID) when the interface is in general mode. Use the `switchport mode general` command to set the VLAN membership mode of a port to “general.” To configure the default value, use the `no` form of this command.

**Syntax**

`switchport general pvid vlan-id`

`no switchport general pvid`

- `vlan-id` — PVID. The VLAN ID may belong to a non-existent VLAN.

**Default Configuration**

The default value for the `vlan-id` parameter is 1 when the VLAN is enabled. Otherwise, the value is 4093.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

Setting a new PVID does NOT remove the previously configured PVID VLAN from the port membership.

**Example**

The following example shows how to configure the PVID for 1/0/8, when the interface is in general mode.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport general pvid 234
```
**switchport mode**

Use the `switchport mode` command in Interface Configuration mode to configure the VLAN membership mode of a port. To reset the mode to the appropriate default for the switch, use the **no** form of this command.

**Syntax**

```
switchport mode {access | trunk | general}
no switchport mode
```

- **access**—An access port connects to a single end station belonging to a single VLAN. An access port is configured with ingress filtering enabled and will accept either an untagged frame or a packet tagged with the access port VLAN. Tagged packets received with a VLAN other than the access port VLAN are discarded. An access port transmits only untagged packets.

- **trunk**—A trunk port connects two switches. A trunk port may belong to multiple VLANs. A trunk port accepts only packets tagged with the VLAN IDs of the VLANs to which the trunk is a member or untagged packets if configured with a native VLAN. A trunk port only transmits tagged packets for member VLANs other than the native VLAN and untagged packets for the native VLAN.

- **general**—Full 802.1Q support VLAN interface. A general mode port is a combination of both trunk and access ports capabilities. It is possible to fully configure all VLAN features on a general mode port. Both tagged and untagged packets may be accepted and transmitted.

**Default Configuration**

The default switchport mode is **access**.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

**User Guidelines**

This command has no user guidelines.
**Example**

The following example configures Gi1/0/5 to access mode.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-Gi1/0/5)#switchport mode access
```

**switchport mode dot1q-tunnel**

Use the `switchport mode dot1q-tunnel` command to enable QinQ tunneling on customer edge (CE) interfaces. Use the `no` form of the command to return the interface to the default switchport mode (access).

**Syntax**

```plaintext
switchport mode dot1q-tunnel
no switchport mode dot1q-tunnel
```

**Default Configuration**

By default, QinQ processing of frames is disabled.

**Command Mode**

Interface mode (physical and port channel), Interface range mode (physical and port channel)

**User Guidelines**

This command configures a customer edge (CE) port for QinQ tunneling. The dot1q-tunnel mode is an overlay on switchport access mode. In particular, configuring the access mode PVID sets the outer dot1q-tunnel VLAN ID. Changing the switchport mode to access, general, or trunk, effectively disables tunneling on the interface.

Customer edge ports can be physical ports or port channels. Untagged frames received on the CE interface will be processed as if they belong to the PVID and will be transmitted out the SP interface with a single VLAN tag. Tagged frames received on the CE interface will be transmitted out the service provider (SP) interface with an outer tag containing the native VLAN ID and the inner tag as received on the CE interface.
CE interfaces must be configured in dot1q-tunnel mode with the PVID configured with the outer tag (native) VLAN ID for the associated service provider (SP) interface. Configure the outer VLAN ID using the `switchport access vlan` command. All MAC address learning and forwarding occurs on the outer VLAN tag. The VLAN ID must be common to both the SP port and the CE ports.

The service provider interface must be configured for egress tagging (trunk or general mode) with a native VLAN identical to the PVID of the associated CE ports. SP interfaces should be configured with a single VLAN ID. A trunk mode port will accept untagged packets on the native VLAN and be a member of any newly created VLANs by default. In general mode, it is possible to directly configure the port to only accept tagged packets with a single VLAN ID.

It is not possible to configure an inner VLAN TPID value. The inner VLAN TPID value is always Ethernet (0x8100).

Multiple groups of associated CE and SP ports can be defined by configuring the groups with unique VLAN IDs.

The port mirroring logic stage occurs after the tag processing stage on ingress and before the tag processing stage on egress. When mirroring packets associated with SP or CE ports, the outer VLAN tag may or may not appear in the frame. Due to the internal processing of QinQ tagging, the TPID of ingress frames mirrored from the SP port will always be 0x8100. In addition, packets forwarded internally across a stacking link may have different tags applied than packets forwarded on a local egress port. This is due to the processing required for forwarding across a stack.

**Example**

This example configures ports Gi1/0/10 through Gi1/0/24 as CE ports using VLAN 10 as the service provider VLAN ID. See the example for the `switchport dot1q ethertype` command to configure an associated SP port.

```
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface range gi1/0/10-24
console(config-if)#switchport access vlan 10
console(config-if)#switchport mode dot1q-tunnel
console(config-if)#exit
```
switchport mode private-vlan

Use the `switchport mode private-vlan` command in Interface Configuration mode to define a private VLAN association for an isolated or community interface or a mapping for a promiscuous interface.

Use the `no` form of the command to remove the private VLAN association or mapping from the interface.

**Syntax**

```
switchport mode private-vlan {host|promiscuous}
```

```
no switchport mode
```

- **host**—Configure the interface as a private VLAN host port. Host ports are community or isolated ports, depending on the VLAN to which they belong.
- **promiscuous**—Configure the interface as a private VLAN promiscuous port. Promiscuous ports are members of the primary VLAN.

**Default Configuration**

This command has no default configuration. By default, a port is neither configured as promiscuous or host.

**Command Mode**

Interface Configuration (physical or port-channel)

**User Guidelines**

Do not configure private VLANs on ports configured with any of these features:

- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- Voice VLAN

It is recommended that the private VLAN host ports be configured as spanning-tree portfast.

**Example**

```
console(config)#interface gigabitethernet 1/0/8
```
console(config-if-Gi1/0/8)#switchport mode private-vlan host

**switchport private-vlan**

Use the `switchport private-vlan` command in Interface Configuration mode to define a private VLAN association for an isolated or community port or a mapping for a promiscuous port.

Use the no form of the command to remove the private VLAN association or mapping from the interface.

**Syntax**

```plaintext
switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id [add|remove] secondary-vlan-list}
no switchport private-vlan {host-association|mapping}
```

- **host-association**—Defines VLAN associations for community or host ports.
- **mapping**—Defines the private VLAN mapping for promiscuous ports.
- **primary-vlan-id**—Primary VLAN ID of a private VLAN.
- **secondary-vlan-id**—Secondary (isolated or community) VLAN ID of a private VLAN.
- **add**—Associates the secondary VLAN with the primary one.
- **remove**—Deletes the secondary VLANs from the primary VLAN association.
- **secondary-vlan-list**—A list of secondary VLANs to be mapped to a primary VLAN.

**Default Configuration**

This command has no default association or mapping configuration.

**Command Mode**

Interface Configuration (physical or port-channel)

**User Guidelines**

This command has no user guidelines.
Example

```plaintext
console(config)#vlan 10,20
console(config-vlan10,20)#exit
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#switchport private-vlan host-association 10 20
```

**switchport trunk**

Use the `switchport trunk` command in Interface Configuration mode to configure VLAN membership for a trunk port or to set the native VLAN for an interface in Trunk Mode.

**Syntax**

```plaintext
switchport trunk {allowed vlan vlan-list | native vlan vlan-id}
no switchport trunk { allowed | native } vlan
```

- **vlan-list**—Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all. The vlan-list format is as follows:
  - all specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
  - add adds the defined list of VLANs to those currently set instead of replacing the list.
  - remove removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form X-Y or X,Y,Z are valid in this command.
  - except lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
  - vlan-atom is either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

- **valid-id**—A valid VLAN id in the range 1–4093. This is the native VLAN for the trunk port and will accept and send traffic on this VLAN in untagged format.
**Default Configuration**

A trunk port is a member of all VLANs by default.

VLAN 1 is the default native VLAN on a trunk port. The default allowed VLAN membership on a trunk port is all VLANs.

**Command Mode**

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

Interface Range mode

Port-Channel Range mode

**User Guidelines**

Untagged traffic received on a trunk port is forwarded on the native VLAN, if configured.

To drop untagged traffic on a trunk port, remove the native VLAN from the trunk port. (Ex. `switchport trunk allowed vlan remove 1`.) Management traffic is still allowed on the trunk port in this configuration.

The no form of the command sets the allowed or native VLAN membership back to the defaults.

It is possible to exclude VLANs that have not yet been created from trunk port membership. For example, it is possible to exclude VLANs learned dynamically via GVRP from being configured on a trunk port using this command.

**Example**

```
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)#switchport trunk allowed vlan 1-1024
console(config-if-Gi1/0/1)#switchport trunk allowed vlan except 1,2,3,5,7,11,13
```

**switchport trunk encapsulation dot1q**

Use this command for compatibility. This command performs no action.

**Syntax**

`switchport trunk encapsulation dot1q`
**Default Configuration**
Dell EMC Networking switches use dot1q encapsulation on trunk ports by default.

**Command Mode**
Interface config mode, Interface range mode (including port-channels)

**User Guidelines**
This command performs no action. Dell EMC Networking switches always use dot1q encapsulation on trunk mode ports.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example demonstrates compatibility.
```
console(config-if-Gi1/0/1)#switchport trunk encapsulation dot1q
```

**vlan**
Use the `vlan` command in Global Configuration mode to configure a VLAN. To delete a VLAN, use the `no` form of this command.

**Syntax**
```
vlan  {vlan-list}
no vlan  {vlan-list}
```

- `vlan–list`—A list of one or more valid VLAN IDs. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 1–4093)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration (Config)
**User Guidelines**
Deleting the VLAN assigned as the PVID on an access port will cause VLAN 1 to be assigned as the PVID for the access port. Deleting the VLAN assigned as the native VLAN for a trunk port will cause the trunk port to discard untagged frames received on the port. Creating a VLAN adds it to the allowed list for all trunk ports except those where it is specifically excluded. Ports and port channels can be configured with VLANs that do not exist. They will not forward traffic on nonexisting VLANs.

**Example**
The following example shows how to create (add) VLAN IDs 22, 23, and 56.
```
console(config)#vlan 22,23,56
```

**vlan association mac**
Use the `vlan association mac` command in VLAN Configuration mode to associate a MAC address to a VLAN. The maximum number of MAC-based VLANs is 256. Only packets with a matching source MAC address are placed in the VLAN.

**Syntax**
```
vlan association mac mac-address
```
```
no vlan association mac mac-address
```

- **mac-address** — MAC address to associate to the VLAN. (Range: Any MAC address in the format xxxx.xxxx.xxxx or xx:xx:xx:xx:xx:xx)

**Default Configuration**
No assigned MAC address.

**Command Mode**
VLAN Configuration mode

**User Guidelines**
This command has no user guidelines.
Example
The following example associates MAC address with VLAN ID 1.

console(config)# vlan 1
console(config-vlan-1)#vlan association mac 0001.0001.0001

vlan association subnet

Use the `vlan association subnet` command in VLAN Configuration mode to associate a VLAN to a specific IP-subnet. Only packets with a matching source IP address are placed into the VLAN.

Syntax

```
vlan association subnet ip-address subnet-mask
no vlan association subnet ip-address subnet-mask
```

- **ip-address** — Source IP address. (Range: Any valid IP address)
- **subnet-mask** — Subnet mask. (Range: Any valid subnet mask)

Default Configuration

No assigned ip-subnet.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example associates the 192.168.0.xxx IP address with VLAN ID 1.

```
console(config)# vlan 1
console(config-vlan-1)#vlan association subnet 192.168.0.0 255.255.255.0
```
**vlan makestatic**

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

**Syntax**

`vlan makestatic vlan-id`

- `vlan-id` — Valid VLAN ID. Range is 2–4093.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration Mode

**User Guidelines**

The dynamic VLAN (created via GRVP) should exist prior to executing this command. See the Type column in output from the `show vlan` command to determine that the VLAN is dynamic.

**Example**

The following changes vlan 3 to a static VLAN.

```
console(config-vlan)#vlan makestatic 3
```

**vlan protocol group**

Use the `vlan protocol group` command in Global Configuration mode to add protocol-based groups to the system. When a protocol group is created, it is assigned a unique group ID number. The group ID is used to identify the group in subsequent commands. Use the `no` form of the command to remove the specified VLAN protocol group name from the system.

**Syntax**

`vlan protocol group group-id`
no vlan protocol group group-id
  • group-id — The protocol-based VLAN group ID, to create a protocol-based VLAN group. To see the created protocol groups, use the show port protocol all command.

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
console(config)# vlan protocol group 1

vlan protocol group add protocol

Use the vlan protocol group add protocol command in Global Configuration mode to add a protocol to the protocol-based VLAN groups identified by groupid. A group may have more than one protocol associated with it. Each interface and protocol combination can be associated with one group only. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group.

To remove the protocol from the protocol-based VLAN group identified by groupid, use the no form of this command.

Syntax
vlan protocol group add protocol group-id ethertype value
no vlan protocol group add protocol group-id ethertype value
  • group-id — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the vlan protocol group command. To see the group ID associated with the name of a protocol group, use the show port protocol all command.
• **ethertype value** — The protocol you want to add. The ethertype value can be any valid hexadecimal number in the range 0x0600 to 0xffff.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays how to add the “ip” protocol to the protocol based VLAN group identified as “2.”

```
console(config)#vlan protocol group add protocol 2 ethertype 0xXXXX
```

**vlan protocol group name**
This is a new command for assigning a group name to vlan protocol group id.

**Syntax**

```
vlan protocol group name group-id groupName
no vlan protocol group name group-id
```

• **groupid**—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the `vlan protocol group` command. To see the group ID associated with the name of a protocol group, use the `show port protocol all` command

• **groupName**—The group name you want to add. The group name can be up to 16 characters length. It can be any valid alpha numeric characters.

**Default Configuration**
This command has no default configuration.
**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
console(config)# vlan protocol group name 1 usergroup

**vlan protocol group remove**

Use the `vlan protocol group remove` command in Global Configuration mode to remove the protocol-based VLAN group identified by groupid.

**Syntax**

```
vlan protocol group remove group-id
```

- **group-id** — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the `vlan protocol group` command. To see the group ID associated with the name of a protocol group, use the `show port protocol all` command.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the removal of the protocol-based VLAN group identified as “2.”

```
console(config)#vlan protocol group remove 2
```
Switchport Voice VLAN Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Voice VLAN feature enables switch ports to carry voice traffic with an administrator-defined priority so as to enable prioritization of voice traffic over data traffic. Using Voice VLAN helps to ensure that the sound quality of an IP phone is protected from deterioration when the data traffic utilization on the port is high.

Voice VLAN is the preferred solution for applying QoS to voice traffic in an enterprise environment. Voice VLAN scales with the number of ports and does not make significant demands on the switch CPU for classification of voice traffic. However, Voice VLAN does require the administrator to perform the additional configuration step of defining the QoS policy to be applied to voice traffic.

The switch can be configured to support voice VLAN on a port connecting to the VoIP phone. When a VLAN is associated with the voice VLAN port, then the VLAN ID information is passed onto the VoIP phone using LLDP-MED. Voice data coming from the VoIP phone is tagged by the phone with the transmitted VLAN ID; regular data arriving on the switch is given the default PVID of the port.

When an IEEE 802.1p priority is associated with the voice VLAN port, then the priority information is passed to the VoIP phone using LLDP-MED. It is expected that the voice data coming from the VoIP phone is tagged with VLAN 0 or the voice VLAN and with the transmitted priority. Configure the voice vlan data priority on the port to enable the switch to transmit the IEEE 802.1p or DSCP values to the phone in the LLDP-MED Network Policy TLV. Regular data arriving on the switch is given the default priority of the port (default 0) and the voice traffic is received with the priority assigned by the phone, allowing the switch to provide distinguished service to the voice traffic.

The switch can be configured to override the voice traffic CoS by entering an internal ACL associated with the MAC address of the IP phone. Alternatively, a diffserv policy can be configured for the voice VLAN which assigns voice traffic to a queue and also remarks the CoS or DSCP values in the voice
traffic. See the User Configuration Guide for more information. Voice VLAN is recommended for enterprise-wide deployment of voice services on the IP network.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport voice vlan</td>
<td>–</td>
</tr>
<tr>
<td>switchport voice vlan (Interface)</td>
<td>authentication event server dead action authorize voice</td>
</tr>
<tr>
<td>switchport voice vlan priority</td>
<td>show voice vlan</td>
</tr>
</tbody>
</table>

**switchport voice vlan**

This command is used to enable the voice VLAN capability on the switch.

**Syntax**

switchport voice vlan
no switchport voice vlan

**Command Mode**

Global Configuration

**User Guidelines**

Voice VLAN must be configured on access or general mode ports. It is not supported on trunk mode ports.

**Command History**

Syntax updated in version 6.5 firmware.

**Default Value**

This feature is disabled by default.
Example
console(config)#switchport voice vlan
console(config)#no switchport voice vlan

switchport voice vlan (Interface)
This command is used to assign the voice VLAN ID on the interface.

Syntax
switchport voice vlan \{vlan-id | dot1p priority | none | untagged | priority extend trust | override-authentication | dscp value\}
no switchport voice vlan [priority extend] [override-authentication]

- **vlan-id**—Configure an existing VLAN as the voice VLAN. This VLAN ID is also sent to the phone via LLDP-MED/CDP unless the none parameter is also specified.
- **dot1p**—Enable LLDP-MED/CDP to configure the phone to send the specified 802.1p priority in voice packets.
- **none**—Do not send LLDP-MED information to the phone. Allow the phone to use it’s own configuration for voice packets.
- **untagged**—Enable LLDP-MED/CDP to configure the phone to send untagged or priority tagged voice traffic.
- **priority extend trust**—Configure the switch to trust the priority of received voice packets. Use the no form of the command to configure the switch to ignore the received priority of voice packets and remark voice VLAN packets.
- **dscp value**—Enable LLDP-MED/CDP to configure the phone to send the specified DSCP value in voice packets.
- **override-authentication**—Allow access to the voice VLAN regardless of the 802.1X port authentication state. Use the no form of the command to require authentication to use the voice VLAN. Use the no form of the command for 802.1X-capable IP phones configured to use 802.1X authentication.
Default Configuration

The default DSCP value is 46. The default CoS is 5 for untrusted ports. The default is tagged voice VLAN traffic. The default data priority is to trust the received CoS value. The default override-authentication value is to require authentication. No voice VLAN ID is configured by default. The default 802.1p value is none.

Command Mode

Interface Configuration (Ethernet) mode.

User Guidelines

Enable voice VLAN using the following steps:

- Create the voice VLAN on the switch.
- Configure the interface in access or general mode.
- Enable voice VLAN globally and on the desired interfaces.
- Optionally configure 802.1X MAC or port-based authentication on the interface and globally.

If using MAC based authentication, also:

- Configure one or more RADIUS servers on the switch.
- Configure the RADIUS servers to send the VSA traffic-class = voice in the Access-Accept.
- Enable 802.1X authentication on the phone.
- Ensure the IP phone connected ports are configured in general mode.
- Optionally enable critical voice VLAN.

If using auto authentication:

- Optionally configure the interface to override authentication. If authentication is not overridden, the IP phone must authenticate using 802.1X.

Voice VLAN may be configured on general or access mode ports. It is not supported on trunk mode ports.

Use the `switchport voice vlan` vlan-id command to enable voice VLAN on an interface.
Voice VLAN information is transmitted to the phone via LLDP-MED in the Network Policy TLV (Application Type Voice, Tagged Yes, …). Voice VLAN information is transmitted to the phone via CDP in the Appliance VLAN TLV. The voice VLAN must be configured on the switch and must be different than the data VLAN. The configured or default priority is sent to the phone Class of Service (CoS) TLV. The trust status is sent to the phone via CDP in the Extended trust TLV. The configured or default priority/DSCP is sent to the phone via LLDP in the MED TLVs. LLDP and CDP packets are exchanged regardless of the 802.1X authentication state.

In MAC-based and auto authentication mode, a voice packet is switched based on the source MAC address of the IP phone. If override authentication is enabled, voice packets received are switched regardless of the 802.1X authentication state. Likewise, voice packets from the switch are transmitted over the port regardless of the 802.1x authentication state when the override option is enabled.

In MAC-based and auto authentication modes, the switch identifies a device as a voice device when an Access-Accept is received from the AAA service with the proprietary VSA device-traffic-class = voice.

When 802.1X authenticates a device onto the voice VLAN using MAC-based authentication, the device is also allowed access over the data VLAN for approximately thirty seconds after authentication succeeds. This allows the device to learn the voice VLAN via non-standard mechanism such as DHCP, HTTP or TFTP.

If trust mode is disabled, the switch remarks the priority and/or DSCP value of received voice VLAN packets to the configured or default values (priority 5 and DSCP 46). If trust mode is enabled, voice packets are not remarked.

If trust mode is disabled, the switch classifies the voice packets into CoS queue 2. If trust mode is enabled, voice packets are classified per the switch configuration.

Use of the override authentication option allows packets to flow over the voice VLAN regardless of the AAA authentication status. The switch cannot distinguish among voice and other packets in the voice VLAN. Use of this option should be carefully considered as it may allow malevolent users unrestricted access to network resources, particularly if MAC-based authentication is not enabled.
The voice VLAN may not be configured as a PVID. The switch enforces this restriction by not configuring the voice VLAN, if the VLAN is the PVID of any port, or by failing the PVID assignment if the VLAN is a voice VLAN.

The voice VLAN may not be configured as the unauthenticated VLAN and vice-versa.

The voice VLAN may not be configured as the guest VLAN and vice-versa.

The voice VLAN may not be configured as a private VLAN host port.

**Command History**

Description updated in 6.3.0.5 release. Syntax updated in release 6.5.1.0.

**Example**

This example configures an interface to use VLAN 100 as the voice VLAN and sends LLDP configuration in the Network Policy TLV to the phone to assign VLAN 100 to 802.1p priority 5. The data priority is trusted by default.

```bash
console(config)#vlan 100
console(config-vlan100)#interface gi1/0/1
console(config-if-Gi1/0/1)#voice vlan 100
console(config-if-Gi1/0/1)#voice vlan dot1p 5
```

In this example, the IP phone will use its own configuration (no policy is sent via LLDP).

```bash
console(config-if-Gi1/0/1)#voice vlan none
console(config-if-Gi1/0/1)#voice vlan untagged
```

This example shows the configuration for a switch with a directly connected IP phone that is not 802.1X capable. All devices will have access to the voice VLAN regardless of the authentication state of the data device.

1. **Create the voice VLAN.**

   ```bash
   console#configure
   console(config)#vlan 25
   console(config-vlan25)#exit
   ```

2. **Enable the Voice VLAN feature on the switch.**

   ```bash
   console(config)#switchport voice vlan
   ```
3 Configure port 10 to be in access mode. The data VLAN ID is 1 and uses untagged packets.

   console(config)#interface gi1/0/10
   console(config-if-Gi1/0/10)#switchport mode access

4 Enable port-based 802.1X authentication on the port for the data traffic.

   console(config-if-Gi1/0/10)#dot1x port-control auto

5 Enable the voice VLAN feature on the interface. Voice packets are tagged using VLAN 25.

   console(config-if-Gi1/0/10)#switchport voice vlan 25

6 Allow access to the voice VLAN regardless of the 802.1X port authentication state.

   console(config-if-Gi1/0/10)#switchport voice vlan override-authentication
   console(config-if-Gi1/0/10)#show voice vlan interface gi1/0/10

   Interface................................. Gi1/0/10
   Voice VLAN Interface Mode............... Enabled
   Voice VLAN ID............................ 25
   Voice VLAN COS Override............... False
   Voice VLAN DSCP Value.................. 46
   Voice VLAN Port Status.................. Disabled
   Voice VLAN Authentication.............. Disabled

**switchport voice vlan priority**

This command is to either trust or not trust (untrust) the data traffic arriving on the voice VLAN port.

**Syntax**

`switchport voice vlan priority {trust | untrust}`

- **trust**—Trust the IEEE 802.1p user priority contained in packets arriving on the voice VLAN port.
• **untrust**—Do not trust the IEEE 802.1p user priority contained in packets arriving on the voice VLAN port. This overrides the received value with the configured 801.2p value. If a distinguished service for voice traffic is required, an ACL or diffserv policy must be configured.

**Command Mode**
Interface Configuration

**Default Value**
trust

**Example**
```bash
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)#voice vlan data priority untrust
console(config-if-Gi1/0/1)#voice vlan data priority trust
```

**authentication event server dead action authorize voice**

Use the `authentication event server dead action authorize voice` command to allow voice VLAN access when no AAA server can be contacted. Use the `no` form of the command to disable voice VLAN access in such cases.

**Syntax**
```
authentication event server dead action authorize voice
no authentication event server dead action authorize voice
```

**Default Configuration**
Critical voice VLAN is disabled by default.

**Command Mode**
Interface Configuration mode (Ethernet)
**User Guidelines**

During authentication, the switch identifies a device as a voice device when an Access-Accept is received from the AAA service with Cisco proprietary VSA device-traffic-class=voice. Phones/devices using the voice VLAN are periodically reauthenticated. If no AAA server is available during reauthentication, access to the voice VLAN is removed when authentication fails.

Critical voice VLAN supports voice VLAN access on an interface connected to an 802.1X-capable host during RADIUS server outages. Use of this command allows traffic to continue to flow over the voice VLAN when no RADIUS server is available to reauthenticate the IP phone. Newly authenticating phones do not have access to the critical voice VLAN service. Only 802.1X-capable devices are eligible for critical voice VLAN treatment. This restriction is not enforced by configuration.

Enable critical voice VLAN using the following steps:

- Create the voice VLAN on the switch.
- Configure the interface in access or general mode.
- Configure MAC based authentication on the interface.
- Configure one or more RADIUS servers on the switch and enable 802.1X globally.
- Configure the RADIUS servers to send the VSA traffic-class=voice in the Access-Accept.
- Enable 802.1X authentication on the phone.
- Enable voice VLAN on the interface and globally.
- Enable critical voice VLAN.

IP phones that bypass authentication (**switchport voice vlan auto override-authentication**) do not interoperate with the critical voice VLAN. If override authentication is enabled, voice packets received are switched, regardless of the 802.1X authentication state. Likewise, voice packets from the switch are transmitted over the port, regardless of the 802.1x authentication state when the override option is enabled.

The voice VLAN must be configured on the interface and must be different than the data VLAN (PVID).
**Command History**
Command introduced in version 6.5 firmware.

**show voice vlan**
This command displays information about the voice VLAN.

**Syntax**
show voice vlan [interface {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port} | all]

**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
- When the `interface` parameter is not specified, only the global mode of the voice VLAN is displayed.
- When the `interface` parameter is specified, the following is displayed:

<table>
<thead>
<tr>
<th>Output Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface ID.</td>
</tr>
<tr>
<td>Voice VLAN Interface Mode</td>
<td>The admin mode of the voice VLAN on the interface.</td>
</tr>
<tr>
<td>Voice VLAN ID</td>
<td>The voice VLAN ID.</td>
</tr>
<tr>
<td>Voice VLAN Priority</td>
<td>The 802.1p priority for the voice VLAN on the port. This is only displayed if configured.</td>
</tr>
<tr>
<td>Voice VLAN Untagged</td>
<td>The tagging option for the voice VLAN traffic.</td>
</tr>
<tr>
<td>Voice VLAN COS Override</td>
<td>The Override option for the voice traffic arriving on the port.</td>
</tr>
<tr>
<td>Voice VLAN Status</td>
<td>The operational status of voice VLAN on the port.</td>
</tr>
</tbody>
</table>

When the **all** parameter is used for the interface, all interfaces are displayed.
Example

(console)#show voice vlan interface gi1/0/1

Interface................................. Gi1/0/1
Voice VLAN Interface Mode................ Enabled
Voice VLAN Priority....................... 2
Voice VLAN COS Override.................. True
Voice VLAN DSCP Value..................... 46
Voice VLAN Port Status..................... Disabled
Voice VLAN Authentication................ Disabled
Security Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Security commands enable network operators to administer security for administrator access to the switch management console or web interface as well as to configure restrictions of network access for network attached devices.

This section of the document contains the following security commands:

<table>
<thead>
<tr>
<th>AAA Commands</th>
<th>Captive Portal Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Profiles Commands</td>
<td>Denial of Service Commands</td>
</tr>
<tr>
<td>E-mail Alerting Commands</td>
<td>Management ACL Commands</td>
</tr>
<tr>
<td>RADIUS Commands</td>
<td>Password Management Commands</td>
</tr>
<tr>
<td>TACACS+ Commands</td>
<td>SSH Commands</td>
</tr>
<tr>
<td>802.1x Commands</td>
<td>—</td>
</tr>
</tbody>
</table>
AAA Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Dell EMC Networking switches support authentication of network users and switch administrators via a number of methods. Management access to the switch is via telnet, HTTP, SSH, or the serial console (SNMP access is discussed in the SNMP Commands section). To ensure that only authorized users can access or change the configuration of the switch, the administrator can require that administrative access be authenticated.

Administrative Authentication

Switch administrators can be authenticated based on:

- Login mode
- Switch access method
- Access to Privileged Exec mode
- Two levels of access:
  - 1 = Read-only
  - 15 = Read-Write

The supported authentication methods for switch management access are:

- Local: The user's locally stored ID and password are used for authentication.
- RADIUS: The user's ID and password are authenticated using the RADIUS server.
- TACACS+: The user's ID and password are authenticated using the TACACS+ server.
- None: No authentication is used.
- Enable: Uses the enable password for authentication.
- Line: Uses the line password for authentication.
- Authentication Preference Lists (APLs): An Authentication Preference List is an ordered list of authentication methods.
To authenticate a switch administrator, the authentication methods in the APL for the access line are attempted in order until an authentication attempt returns a success or failure return code. If a method times out, the next method in the list is attempted. The component requesting authentication is unaware of the ultimate authentication source. If a method in the preference list does not support the concept of time-out, subsequent entries in the list are never attempted. For example, the local authentication method implementation does not supply a time-out value. If a list contains the local method, followed by the RADIUS authentication method, the RADIUS method is not attempted.

Once an APL is created, a reference to that APL can be stored in the access line configuration to determine how specific components should authenticate users. The APL and associated component ID are stored together. A single APL can be referenced by multiple methods.

The administrator can enable/disable/reorder authentication methods on a per method basis (see above).

### Administrative Accounting

The administrator may choose to account administrative activity on the switch. The following accounting types are supported:

- **User exec sessions**: User login and logout times are noted and conveyed to an external AAA server.
- **User executed commands**: Commands executed by the user and the time of execution are accounted and conveyed to an external AAA server.

Administrator activity can be accounted for at the end and/or at the beginning of the activity. For this purpose, the following record-types are defined:

- **Start-stop**
  
  Accounting notifications are sent when the administrator logs into the switch and when the administrator exits exec mode. Accounting notifications are also sent at the beginning and at the end of each administrator executed command. Command execution does not wait for the accounting notification to be recorded at the AAA server.

- **Stop-only**
Accounting notification is sent when the administrator exits exec mode. The duration of the exec session is logged in the accounting notice. Accounting notifications are sent at the end of each administrator executed command. In the case of commands like `reload`, and `clear config`, an exception is made and the stop accounting notice is sent at the beginning of the command.

### Accounting Method Lists

An Accounting Method List (AML) is an ordered list of accounting methods that can be applied to the accounting types (exec or commands). Accounting Method Lists are identified by the `default` keyword or by a user-defined name. TACACS+ and RADIUS are supported as accounting methods. TACACS+ accounts all accounting types (exec and commands). RADIUS only accounts exec sessions.

### Access Line Modes

AMLs can be applied to the following access line modes for accounting purposes:

- **Console**: This mode is used when user logs in to the switch using serial console.
- **Telnet**: This mode is used when user logs in through Telnet.
- **SSH**: This mode is used when user logs in through SSH.

By default, no accounting is enabled for any line Configuration modes. The following default Accounting Methods List are available.

<table>
<thead>
<tr>
<th>Default List Name</th>
<th>Accounting Type</th>
<th>Record Type</th>
<th>Accounting Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Exec List</td>
<td>exec</td>
<td>Start-stop</td>
<td>TACACS+</td>
</tr>
<tr>
<td>Default Command List</td>
<td>commands</td>
<td>Stop-only</td>
<td>TACACS+</td>
</tr>
</tbody>
</table>

The default lists are not applied to any line-configuration modes by default. See `Line Commands` for information on associating an accounting method list (AML) to a login session (console, SSH, Telnet).
Command Authorization

Dell EMC Networking switches support per command or enable authorization using a TACACS server. See the authorization command in this section for further information. Additionally, the RADIUS or TACACS server can be configured to assign an administrative profile to a switch administrator. The administrative profile identifies groups of commands which may be executed by the administrator. See the Administrative Profiles Commands section for further information on this capability.

Network Authentication

The network administrator can require that devices attached to the network be authenticated prior to gaining access to network resources. This is most often performed by the use of IEEE 802.1x in conjunction with a RADIUS or TACACS authentication server. Dell EMC Networking switches support use of RADIUS or TACACS authentication servers as well as a local, switch based, authentication server. Refer to the RADIUS Commands section for information on configuring a RADIUS server for authentication of network devices. See the 802.1x Commands section for information on configuring device access to network resources.

Dell EMC Networking switches support an internal authentication capability that allows configuration of authentication preference lists for network connected devices. The authentication preference lists support authentication methods such as IEEE 802.1x, internal authentication, and no authentication. MAC Authentication Bypass may be configured to allow IEEE 802.1x unaware devices access to the network. Refer to the section below for information on configuring authentication preference lists for network device access.

Local 802.1x Authentication Server

The Dell EMC Networking switch supports a dedicated database for local authentication of users for network access through the 802.1x feature. This functionality is distinct from management access for the switch. See the 802.1x Commands section for information on configuring IEEE 802.1x access to the network using an external authentication server.
The Internal Authentication Server feature provides support for the creation of users for IEEE 802.1x access only, i.e. without switch management access. This feature maintains a separate database of users allowed for 802.1x access.

The authentication method `ias` is available in the list of methods supported by authentication to support user database lookup. The `ias` method cannot be added in the same authentication list that has other methods like local, radius and reject.

Whenever an operator configures a port in 802.1x authentication mode and selects the authentication method as `ias`, then the user credentials received from the 802.1x supplicant are validated against the user database by the 802.1x component. The 802.1x application accesses the 802.1x user database to check whether the user credentials present in the authentication message corresponds to a valid user or not. If so then an event is generated which triggers the 802.1x state machine to send a challenge to the supplicant. Otherwise a failure is returned to the 802.1x state machine and the user is not granted access to the port.

If user(s) credentials are changed, the existing user connection(s) are not disturbed and the changed user(s) credentials are only used when a new EAP request arises.

A CLI configuration mode is added in order to configure 802.1x users and their attributes. The 802.1x maintained user database can also be exported (uploaded) or imported (downloaded) to/from a central location using a TFTP server. Use the `aaa ias-user username` command to add users to the internal database.

**MAC Authentication Bypass**

Today, IEEE 802.1x has become the recommended port-based authentication method at the access layer in enterprise networks. However, there may be 802.1x unaware devices such as printers, fax-machines, etc., that would require access to the network without 802.1x authentication. MAC Authentication Bypass (MAB) is a supplemental authentication mechanism to allow 802.1x unaware clients to authenticate to the network. It uses the 802.1x infrastructure. MAB cannot be supported independently of the 802.1x component.
MAC Authentication Bypass (MAB) provides 802.1x unaware clients controlled access to the network using the devices’ MAC address as an identifier. This requires that the known and allowable MAC address and corresponding access rights be prepopulated in the authentication server. MAB only works when the port control mode of the port is MAC-based and switch port mode is General.

Port access by MAB clients is allowed via local authentication if the user database has corresponding entries added for the MAB clients with user name and password attributes set to the MAC address of MAB clients. Alternatively, a RADIUS authentication server can be configured with the MAC addresses of the MAB clients. In this configuration, the switch uses EAP-MD5, CHAP, and PAP authentication to communicate with the authentication server. No other authentication or privacy protocol is supported for server side authentication.

**Guest VLAN**

The Guest VLAN feature allows a Dell EMC Networking switch to provide a distinguished service to unauthenticated network devices (not rogue devices that fail authentication). This feature provides a mechanism to allow network devices to have network access to reach an external network while restricting their ability to access the internal LAN.

When a client that does not support 802.1x is connected to an unauthorized port that is 802.1x-enabled, the client does not respond to the 802.1x requests from the switch. The port remains in the unauthorized state and the client is not granted access to the network. If a guest VLAN is configured for that port, then the port is placed in the configured guest VLAN, and the port is moved to the authorized state, allowing network access to the client over the guest VLAN. RADIUS accounting records are not transmitted for 802.1X client placed into guest VLAN.

**Unauthenticated VLAN**

The Unauthenticated VLAN feature allows a Dell EMC Networking switch to provide a distinguished service to unauthorized network devices that attempt and fail authentication. This feature provides a mechanism to allow network devices to have network access to an external network while restricting their ability to access the internal LAN.
When a client network device that supports 802.1x is connected to an unauthorized port that is 802.1x enabled with no unauthenticated VLAN configured and the client attempts and fails to authenticate, the port remains in the unauthorized state and the client is not granted access to the network. If an unauthenticated VLAN is configured for the port and the 802.1x client fails to authenticate for the configured number of attempts, the port is placed in the authorized state on the unauthenticated VLAN and the client is granted access to the network.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting</td>
<td>authentication order</td>
<td>show aaa statistics</td>
<td></td>
</tr>
<tr>
<td>aaa accounting delay-start</td>
<td>authentication priority</td>
<td>show accounting methods</td>
<td></td>
</tr>
<tr>
<td>aaa accounting update</td>
<td>authentication restart</td>
<td>show accounting update</td>
<td></td>
</tr>
<tr>
<td>aaa authentication dot1x</td>
<td>clear (IAS)</td>
<td>show authentication</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa authentication enable</td>
<td>clear authentication statistics</td>
<td>show authentication</td>
<td>authentication-history</td>
</tr>
<tr>
<td></td>
<td>authentication-history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>enable password</td>
<td>show authentication</td>
<td>statistics</td>
</tr>
<tr>
<td>aaa authorization</td>
<td>ip http authentication</td>
<td>show authorization methods</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa authorization network</td>
<td>ip https authentication</td>
<td>show users accounts</td>
<td></td>
</tr>
<tr>
<td>default radius</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa ias-user username</td>
<td>password (AAA IAS User</td>
<td>show users login-history</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>password (User Exec)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa server radius dynamic-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>author</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication enable</td>
<td>show aaa ias-users</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>username unlock</td>
<td></td>
</tr>
</tbody>
</table>
aaa accounting

Use this command to configure an accounting method list for User Exec sessions, user-executed commands or 802.1X or to enable accounting. The no version of the command deletes the accounting method list.

Use the no form of the command to delete an accounting method list or disable accounting.

Use either the aaa accounting dot1x default none or no aaa accounting command to disable dot1x accounting.

Syntax

```
aaa accounting {exec | commands | dot1x} {default | list-name} {start-stop | stop-only | none} {radius|tacacs|radius tacacs|tacacs radius}
```

- **exec**—Provides accounting for a User Exec terminal sessions.
- **commands**—Provides accounting for all user executed commands.
- **dot1x**—Provides accounting for DOT1X user commands. Only the default method is available for dot1x.
- **default**—The default list of methods for accounting services.
- **list-name**—Character string used to name the list of accounting methods.
- **start-stop**—Sends a start accounting notice at the beginning of a process, and a stop accounting notice at the end of a process.
- **stop-only**—Sends a stop accounting notice at the end of the requested user process.
- **none**—Disables accounting services on this line or for 802.1X.
- **method**—Use either TACACS or RADIUS server for accounting purposes.

Default Configuration

Accounting is not enabled by default.

Command Mode

Global Configuration
**User Guidelines**

An accounting list is identified by the `default` keyword or a user-specified `list_name`. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end of the session (`start-stop`) or only at the end (`stop-only`). If `none` is specified, accounting is disabled for the specified list. If `tacacs` is specified as the accounting method, accounting records are transmitted to a TACACS+ server. If `radius` is the specified accounting method, accounting records are transmitted to a RADIUS server.

Note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for RADIUS. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type.
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for RADIUS accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for 802.1X accounting.
- For the same set of accounting type and list name, the administrator can change the record type or the methods list, without having to first delete the previous configuration.
- Interim accounting is enabled using the `aaa accounting update` command.
- Use either the `aaa accounting dot1x default none` or `no aaa accounting dot1x default` command to disable dot1x accounting.
- Use the `no aaa accounting exec` or `no aaa accounting` commands to disable aaa accounting and optionally delete an accounting method list.

**Example**

The following shows several examples of the command.

```
(console)#configure
(console-config)#aaa accounting commands default stop-only tacacs
```
(console-config)#aaa accounting exec default start-stop radius
(console-config)#aaa accounting dot1x default start-stop radius
(console-config)#aaa accounting dot1x default none
(console-config)#exit

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration. The first `aaa` command creates a method list for exec sessions with the name ExecList, with record-type as stop-only and the method as TACACS+. The second command changes the record type to start-stop from stop-only for the same method list. The third command for the list changes the methods list to `{tacacs,radius}` from `{tacacs}`.

(console)#configure
(console-config)#aaa accounting exec ExecList stop-only tacacs
(console-config)#aaa accounting exec ExecList start-stop tacacs
(console-config)#aaa accounting exec ExecList start-stop tacacs radius
(console-config)#exit

This example shows how to enable dot1x accounting to RADIUS server for start, interim and stop reports. Interim reports are sent every 60 minutes.

(console)#configure
(console-config)#aaa accounting dot1x default start-stop radius
(console-config)#aaa accounting update periodic 60

The following shows an example of the no version of the command.

(console)#configure
(console-config)#aaa accounting commands userCmdAudit stop-only tacacs
(console-config)#no aaa accounting commands userCmdAudit
(console-config)#exit

**aaa accounting delay-start**

Use the `aaa accounting delay-start` command to delay the sending of Acct-Start packets to RADIUS accounting server(s).

**Syntax**

`aaa accounting delay-start [extended-time delay_value]`

`no aaa accounting delay-start`

- delay_value—The maximum number of seconds to wait before sending the Acct-Start packet to the RADIUS accounting server. Range: 1 to 300 seconds.
Default Configuration
By default, the switch will wait up to the maximum of maximum number of retries (radius server retransmit) multiplied by the timeout (radius server timeout).

Command Mode
Global Configuration mode

User Guidelines
Dell EMC recommends that a fixed time be configured for the delay in order to ensure timely delivery of Acct-Start packets to the RADIUS accounting server. Acct-Interim and Acct-Stop messages are not delayed, nor are any Authentication messages delayed by configuration of this command.

If the switch discovers that the host has obtained an IPv4/IPv6 address, it may send the Acct-Start packet before the expiry of the delay period.

The delay is accounted for in the Acct-Delay-Time attribute sent to the RADIUS accounting server.

Use the show dot1x clients command to display the discovered IPv4 address/IPv6 address received from RADIUS server, if any.

Command History
Command introduced in firmware release 6.5.2.

aaa accounting update
Use the aaa accounting update command to enable the sending of interim accounting packets to RADIUS accounting server(s).

Syntax
aaa accounting update {[newinfo][periodic minutes]}
no aaa accounting update

• periodic minutes—The number of minutes to wait before sending the Interim-Update packet to the RADIUS accounting server. The range for minutes is from 1 to 10081.
• newinfo—Send the Interim-Update packet to the RADIUS accounting server whenever new information is available.

Default Configuration
By default, the sending of Interim-Update packets is disabled. There is no default time period.

Command Mode
Global Configuration mode

User Guidelines
User of the newinfo keyword can cause congestion if many accounted sessions are present on the switch.
The Interim-Update packet contains the accounting information recorded for the user session since the last time an accounting record was sent.
If both the periodic and newinfo keywords are configured, Interim-Update messages are sent whenever new information is available and when the periodic timer expires.
Use the show dot1x clients command to display the discovered IPv4 address/IPv6 address received from the RADIUS server, if any.

Command History
Command introduced in firmware release 6.5.2.

aaa authentication dot1x default
Use the aaa authentication dot1x default command in Global Configuration mode to specify an authentication method for 802.1x clients to access network resources. Use the no form of the command to return the authentication method to its default settings.

Syntax
aaa authentication dot1x default {radius | ias | none}
no aaa authentication dot1x default
  • radius—Uses the RADIUS server(s) for authentication.
• **ias**—Uses the internal authentication server. Only EAP-MD5 authentication is supported for the internal authentication server.

• **none**—Uses no authentication.

**Default Configuration**

No default authentication method is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Only one authentication method may be specified in the command. For the RADIUS authentication method, if the RADIUS server cannot be contacted, the supplicant fails authentication. The **none** method always allows access. The **ias** method utilizes the internal authentication server. The internal authentication server only supports the EAP-MD5 method.

**Example**

The following example configures 802.1x authentication to use no authentication. Absent any other configuration, this command allows all 802.1x users to pass traffic through the switch.

```
console(config)# aaa authentication dot1x default none
```

The following example configures 802.1x authentication to use a RADIUS server. A RADIUS server must be configured previously using the **radius server host auth** command for the radius method to succeed.

```
console(config)#aaa authentication dot1x default radius
```

**aaa authentication enable**

Use the **aaa authentication enable** command in Global Configuration mode to set authentication for accessing higher administrator privilege levels when logged in to the switch console. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
aaa authentication enable {default | list-name} {method1 [method2...]}
```
no aaa authentication enable {default | list-name}

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- **list-name** — Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-15 characters)
- **method1 [method2...]** — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Configuration**

The default enable list is `enableList`. It is used by console, telnet, and SSH and only contains the method `enable` and `none`.

**Command Mode**

Global Configuration mode

**User Guidelines**

The default and optional list names created with the `aaa authentication enable` command are used with the `enable authentication` command.

Create a list by entering the `aaa authentication enable list-name method` command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails to authenticate the administrator. Only the RADIUS or TACACS methods can return an error. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.
To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. Note that enable will not succeed for a privilege level one administrator if no authentication method is defined. A privilege level one administrator must authenticate to get to Privileged Exec mode.

NOTE: Requests sent by the switch to a RADIUS server include the username "$enabx$", where x is the requested privilege level in decimal. For enable to be authenticated on RADIUS servers, add "$enabx$" users to them. The login user ID is also sent to TACACS+ servers for enable authentication.

Example
The following example configures enable authentication to use the enable method for accessing higher privilege levels.

```
console(config)# aaa authentication enable default enable
```

**aaa authentication login**

Use the `aaa authentication login` command in Global Configuration mode to create and enable the authentication method required for administrative access to the switch. To return to the default configuration and optionally delete an authentication list, use the `no` form of this command.

**Syntax**

```
aaa authentication login {default | list-name} {method1 [method2...]}  
no aaa authentication login {default | list-name}
```

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when an administrator logs in.
- **list-name** — Character string used to name the list of authentication methods activated when an administrator logs in to the switch. (Range: 1-15 characters)
- **method1 [method2...]** — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Use the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Use the line password for authentication.</td>
</tr>
</tbody>
</table>
### Default Configuration

The default login lists are `defaultList` and `networkList`. `defaultList` is used by the console and only contains the method `none`. `networkList` is used by telnet and SSH and only contains the method `local`.

### Command Mode

Global Configuration mode

### User Guidelines

The default and optional list names created with the `aaa authentication login` command are used with the `login authentication` command. Create a list by entering the `aaa authentication login` list-name method command for a particular protocol, where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are attempted only if the previous method returns an error, not if there is an authentication failure. Only the RADIUS, TACACS+, local and enable methods can return an error. To ensure that authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down. If specified, `none` must be the last method in the list.

**NOTE:** Auth-Type:=Local does not work for recent versions of FreeRadius. FreeRadius ignores the configuration if Local is used. Administrators should remove Auth-Type=Local and use the PAP or CHAP modules instead.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Use the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Use no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Use the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Keyword Source or destination**

- **local**: Use the local username database for authentication.
- **none**: Use no authentication.
- **radius**: Use the list of all RADIUS servers for authentication.
- **tacacs**: Use the list of all TACACS+ servers for authentication.
Example
The following example configures the default authentication login to attempt RADIUS authentication, then local authentication, then enable authentication, and then, if all the previous methods returned an error, allows the administrator access to the switch console (via the none method).

```text
console(config)# aaa authentication login default radius local enable none
```

aaa authorization
Use the `aaa authorization` command to enable authorization and optionally create an authorization method list. A list may be identified by a user-specified `list-name` or the keyword `default`.

Use the `no` form of the command to disable authorization and optionally delete an authorization list.

Syntax

```
aaa authorization {commands|exec|network} {default|list-name} {method1 [method2]}
```

```
no aaa authorization {commands|exec|network} {default|list-name}
```

- **exec**—Provides Exec authorization. All methods are supported.
- **commands**—Performs authorization of user commands. Only none and TACACs methods are supported.
- **network**—Performs RADIUS authorization. Only the default list is supported.
- **default**—The default list of methods for authorization services. The list `dfltCmdAuthList` is the default list for command authorization and the list `dfltExecAuthList` is the default list for Exec authorization.
- **list-name**—Character string used to name the list of authorization methods. The list name can consist of any alphanumeric character up to 20 characters in length. Use quotes around the list name if embedded blanks are contained in the list name.
- **method**—The following authorization methods are supported:
  - local—Perform local authorization.
  - none—Do not perform authorization. All functions are authorized.
– radius—Request authorization from the configured RADIUS servers.
– tacacs—Request authorization from the configured TACACS+ servers.

**Default Configuration**

When authorization is enabled, the switch attempts to authorize the listed function using the configured method.

Authorization is not enabled by default. Authorization supports Exec authorization and network authorization for RADIUS. Only TACACS is supported for command authorization. Setting a `none` or `local` method for authorization authorizes Exec access for all functions.

The following default Authorization Methods List is present by default:

<table>
<thead>
<tr>
<th>Default List Name</th>
<th>Description</th>
<th>Authorization Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfltCmdAuthList</td>
<td>Default Command List</td>
<td>None</td>
</tr>
<tr>
<td>dfltExecAuthList</td>
<td>Default Exec list</td>
<td>None</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration mode

**User Guidelines**

A maximum of five authorization method lists may be created for exec and command types. The default methods may not be deleted.

When command authorization is configured for a line mode, the switch sends information about the entered command to the AAA server. The AAA server validates the received command and responds with a PASS or FAIL. If a PASS response is received, the command is executed. If a FAIL response is received, the command is not executed and a message is displayed to the user.

Command authorization attempts authorization for all Exec mode commands associated with a privilege level, including global configuration commands. Exec authorization attempts authorization when a user attempts to enter Privileged Exec mode.
When exec authorization is configured for a line mode, the use may not be required to use the `enable` command to enter Privileged Exec mode. If the authorization response indicates the user has privileges for Privileged Exec mode, then the switch bypasses User Exec mode entirely.

If multiple authorization methods are listed, the switch will attempt communication with each method in order, until successful communication is established or all methods in the list have been tried. If authorization fails, then the command is denied and no further attempts at authorization are made for the user request.

If no authorization server is available or configured, the function is denied unless the none method is configured in the list. If authorization is configured on the console, this can lead to situations where the console denies administrative access. Therefore, it is recommended that the console authorization only be enabled with due regard to the risks involved. If none is configured as the last method after radius or tacacs, no authorization is performed if the RADIUS/TACACS servers are down.

The various utility commands like `tftp`, `ping`, outbound `telnet` also must pass command authorization. Applying a script is treated as a single command `apply script` which also must pass authorization. Startup-config commands applied on device boot-up are not subject to the authorization process.

Refer to the **Line Commands** section for information on configured an authorization method for a particular type of line access.

<table>
<thead>
<tr>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>The local method is not supported for command authorization. This method is equivalent to selecting the none method when used for Exec authorization.</td>
</tr>
<tr>
<td>TACACS</td>
<td>Selects TACACS for command or exec authorization.</td>
</tr>
<tr>
<td>None</td>
<td>Selecting the none method authorizes all commands. This option is valid for both command and Exec authorization.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>The radius method is valid for Exec authorization and Network authorization. Network and Exec authorization with RADIUS will work only if the applied authentication method is radius.</td>
</tr>
</tbody>
</table>
Example

Per command authorization example for telnet access using TACACS:

Configure the Authorization Method list.

```bash
console(config)#aaa authorization commands telnet-list tacacs
```

Apply the AML to an access line mode (telnet):

```bash
console(config)#line telnet
console(config-telnet)#authorization commands telnet-list
```

Exec authorization example for SSH using RADIUS with a fallback to the none method:

Configure the Authorization Method list.

```bash
console(config)#aaa authorization exec exec-list radius none
```

Apply the AML to an access line mode (SSH):

```bash
console(config)#line ssh
console(config-ssh)#authorization exec exec-list
```

Display the authorization methods:

```bash
console#show authorization methods
Exec Authorization List       Methods
----------------------------   ------------------------------
dfltExecAuthList              none
exec-list                      radius  none

Command Authorization List    Methods
----------------------------   ------------------------------
dfltCmdAuthList               none
telnet-list                    tacacs

Line       Exec Method Lists      Command Method Lists
---------  ---------------------  ---------------------
Console    dfltExecAuthList       dfltCmdAuthList
Telnet     dfltExecAuthList       telnet-list
SSH        exec-list              dfltCmdAuthList

Network Authorization    Methods
----------------------------  -------
Dot1x                        none
aaa authorization network default radius

Use the `aaa authorization network default radius` command in Global Configuration mode to enable the switch to authorize VLAN assignment by the RADIUS server.

**Syntax**

aaa authorization network default radius
no aaa authorization network default radius

**Default Configuration**

By default, the switch does not accept VLAN assignments by the RADIUS server.

**Command Mode**

Global Configuration mode

**User Guidelines**

The RADIUS server can place a port in a particular VLAN based on the result of the authentication. VLAN assignment must be configured on the external RADIUS server using the RADIUS TUNNEL-TYPE attribute and others. See RADIUS Commands and Security Commands for further information.

If the port is configured to use 802.1X MAC-based authentication and the port is configured as a general mode port, each authenticating data device is placed into the assigned VLAN. Device packets are identified by their source MAC address.

If the port is configured to use 802.1X auto authentication and the port is configured as an access mode port, the PVID of the port is updated for the first data device authentication. Only the first assignment of the PVID takes effect. All subsequent valid authentications will be placed into the first PVID assigned, regardless of the received VLAN ID.

RADIUS-assigned VLANs may be dynamically created. Use the `dot1x dynamic-vlan enable` command to enable dynamic VLAN creation.
Example
The following example enables RADIUS-assigned VLANs.

```
console(config)#aaa authorization network default radius
```

**aaa ias-user username**

Use the `aaa ias-user username` command in Global Configuration mode to configure IAS users and their attributes. Username and password attributes are supported. The ias-user name is composed of up to 64 alphanumeric characters. This command also changes the mode to a user Configuration mode. Use the `no` form of this command to remove the user from the internal user database.

**Syntax**

```
aaa ias-user username user
no aaa ias-user username user
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration

**User Guidelines**

This command has no user guidelines.

**Examples**

```
console#configure
console(config)#aaa ias-user username client-1
console(config-ias-user)#exit
console(config)#no aaa ias-user username client-1
```

**aaa new-model**

The `aaa new-model` command in Global Configuration mode is a no-op command. It is present only for compatibility purposes. Dell EMC Networking switches only support the new model command set.
Syntax
aaa new-model

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
The following example configures the switch to use the new model command set.
console(config)# aaa new-model

aaa server radius dynamic-author
Use this command to enter dynamic RADIUS server configuration mode.

Syntax
aaa server radius dynamic-author

Default Configuration
By default, no dynamic RADIUS servers are configured.

Command Mode
Global Configuration

User Guidelines
Configuring a dynamic RADIUS server causes the system to begin listening on the default port 3799 for RADIUS CoA requests. The switch ensures that a unique session key is sent to the RADIUS server in all Access-Request packets. The Acct-Session-Id, User-Name, and Calling-Station-Id, Framed-
IP-Address, NAS-IP-Address (if configured in switch), NAS-Port identifiers are maintained in the switch for 802.1X session identification. CoA-Request requests must contain at least one of the Acct-Session-Id, Framed-IP-Address, User-Name, or Calling-Station-Id for presentation to the NAS for CoA requests.

A valid authenticated RFC 3575 Disconnect-Request terminates the session without disabling the port. The termination may cause the host to attempt to reauthenticate on the port. If an ACL was applied for the session, the ACL is removed when the session is terminated.

If a valid authenticated RFC 3575 Disconnect-Request request is received from a configured server and the session cannot be found, the switch returns a CoA-NAK message with the 503 Session Context Not Found response code.

If it expected that more than one session will authenticate over a port, use of MAC based authentication is recommended. If MAC based authentication is enabled, the user is denied access to the port even if a previous authentication has occurred on the port.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

The following example configures RADIUS servers at 1.1.1.1, 2.2.2.2, and 3.3.3.3 and CoA clients at 4.4.4.4 and 5.5.5.5. It sets the front panel ports to use 802.1x MAC-based authentication. CoA is configured for two dynamic RADIUS servers located at 1.1.1.1 and 2.2.2.2 using a global shared secret and a third server using a server specific shared secret. CoA and disconnect requests are accepted from the CoA clients at 4.4.4.4 and 5.5.5.5. Any attribute contained in the Disconnect request is allowed for session identification. In this example, the NAS-IP-Address is optionally configured at the fixed IPv4 address of 3.3.3.3. CoA client 5.5.5.5 uses the global server key while client 4.4.4.4 uses a client-specific server key.

```
console#configure terminal
console(config)# aaa new-model
console(config)# aaa authentication dot1x default radius
console(config)# dot1x system-auth-control
console(config)# interface range gi1/0/1-24
console(config-if)# dot1x port-control mac-based
console(config-if)# exit
```
authentication enable

Use this command to globally enable the Authentication Manager. Interface configuration set with the authentication order command takes effect only if the Authentication Manager is enabled.

Use the no form of this command to disable the Authentication Manager.

Syntax
authentication enable
no authentication enable

Default Configuration
The default value is Disabled.

Command Mode
Global Configuration mode
**User Guidelines**

The administrator must ensure that any methods configured by the Authentication Manager are enabled (e.g. enable IEEE 802.1x using the `dot1x system-auth-control` command). Enable MAB using the `dot1x mac-auth-bypass` command.

**Example**

```
console(config)# authentication enable
```

**authentication order**

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Use the `no` form of this command to return the port to the default authentication order.

**Syntax**

```
authentication order {dot1x [mab][captive-portal] | mab [dot1x] [captive-portal] | captive-portal}
no authentication order
```

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Interface Configuration (Ethernet) mode

**User Guidelines**

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.
Example
console(config-if-Gi1/0/1)# authentication order dot1x mab captive-portal
console(config-if-Gi1/0/1)# no authentication order

authentication priority
Use this command to set the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority decides if a previously authenticated client is reauthenticated with a higher-priority method when the same is received. Captive portal is always the last method in the list.
Use the no form of this command to return the port to the default order of priority for the authentication methods.

Syntax
authentication priority {[dot1x|mab|captive-portal] [mab|dot1x|captive-portal] [mab|dot1x|captive-portal]}
no authentication priority

Default Configuration
There is no default configuration for this command.

Command Modes
Interface Configuration (Ethernet) mode.

User Guidelines
Each method can only be entered once. There are no restrictions on the priority ordering of methods.

Example
console(config-if-Gi1/0/1)# authentication priority mab dot1x captive-portal
console(config-if-Gi1/0/1)# no authentication priority
**authentication restart**

Use this command to set the interval after which reauthentication starts. This timer starts only if all the authentication methods fail.

Use the `no` form of this command to set the authentication restart timer to factory default value.

**Syntax**

```
authentication restart time
no authentication restart
```

- `time`—The time, in seconds, after which reauthentication starts, if all the authentication methods have failed. Range: 300-65535.

**Default Configuration**

The default timer value is 300 seconds.

**Command Modes**

Interface Configuration (Ethernet) mode

**User Guidelines**

None

**Example**

```
console(config-if-Gi1/0/1)# authentication restart 1800

console(config-if-Gi1/0/1)# no authentication restart
```

**clear (IAS)**

Use the `clear aaa ias-users` command to delete all IAS users.

**Syntax**

```
clear aaa ias-users
```

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged Exec mode

User Guidelines
There are no user guidelines for this command.

Example
console#clear aaa ias-users

clear authentication statistics
Use this command to clear the authentication statistics.

Syntax
clear authentication statistics {interface-id | all}

Default Configuration
There is no default configuration for this command.

Command Modes
Privileged Exec mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)# clear authentication statistics Gi1/0/1

Are you sure you want to clear authentication manager port stats? (y/n)

clear authentication authentication-history
Use this command to clear the authentication history logs.

Syntax
clear authentication authentication-history {interface-id | all}
• interface-id—The interface.
• all—All interfaces.

Default Configuration
There is no default configuration for this command.

Command Modes
Privileged Exec mode

User Guidelines
None

Example
console(config)# clear authentication authentication-history Gi1/0/1

enable password

Use the enable password command in Global Configuration mode to set a local password to control access to the privileged Exec mode. To remove the password requirement, use the no form of this command.

Syntax
enable password password [encrypted]
no enable password

• password — Password for this level (Range: 8-64 characters). The special characters allowed in the password include ! # $ % & ' ( ) * + , - . / ; < = > @ [ \ ] ^ _ ` { | } ~. User names can contain blanks if the name is surrounded by double quotes. To use the ! character as part of the username or password string, it should be enclosed within quotation marks. For example, username “test!xyz” password “test!xyz”.

• encrypted — Encrypted password entered, copied from another switch configuration.

Default Configuration
This command has no default configuration.
Command Mode
Global Configuration mode

User Guidelines
The Dell EMC Networking firmware emulates industry standard behavior for enable mode authentication over SSH and telnet. The default enable authentication method for telnet and SSH uses the enableNetList method, which requires an enable password. If users are unable to enter privileged mode when accessing the switch via telnet or SSH, the administrator will need to either change the enable authentication method, e.g. to enableList, or set an enable password. If the encrypted parameter is specified, the password parameter is stored as entered in the running-config. No attempt is made to decode the encrypted password. To use the ! character as part of the username or password string, it should be enclosed within quotation marks. For example, username “test!xyz” password “test!xyz”.

Example
The following example defines password “xxxyyyzzz” to control access to user and privilege levels.

```
console(config)# enable password xxxyyyzzz
```

ip http authentication
Use the ip http authentication command in Global Configuration mode to specify authentication methods for http server users. To return to the default, use the no form of this command.

Syntax
ip http authentication {method1 [method2...]}
no ip http authentication

• method1 [method2...] — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>
Default Configuration

The local user database is checked. This action has the same effect as the command `ip http authentication local`.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Example

The following example configures the http authentication.

```
console(config)# ip http authentication radius local
```

**ip https authentication**

Use the `ip https authentication` command in Global Configuration mode to specify authentication methods for users authenticating over HTTPS. To return to the default configuration, use the `no` form of this command.

Syntax

```
ip https authentication {method1 [method2...]}  
no ip https authentication
```

- `method1 [method2...]` — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>
Default Configuration

The local user database is checked. This action has the same effect as the command `ip https authentication local`.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. If `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

When using a Cisco ACS with TACACS+ as the authentication method for HTTPS, the Cisco ACS must be configured to allow the `shell` service. In addition, for admin privileges, the `privilege level` attribute must be set to 15.

Example

The following example configures HTTPS authentication.

```
console(config)# ip https authentication radius local
```

password (AAA IAS User Configuration)

Use the `password` command in aaa IAS User Configuration mode to configure a password for an IAS user. The password is composed of up to 64 alphanumeric characters. An optional parameter `[encrypted]` is provided to indicate that the password given to the command is already pre-encrypted. To clear the user’s password, use the `no` form of this command.
**Syntax**

password password [encrypted]

no password

- password — Password for this level. (Range: 1-64 characters)
- encrypted — Encrypted password to be entered, copied from another switch configuration.

**Default Configuration**

This command has no default configuration.

**Command Mode**

AAA IAS User Configuration

**User Guidelines**

IAS user accounts are distinct from user (administrator) accounts. IAS accounts give access to network resources (via 802.1X or MAB), whereas user accounts give administrative access to the switch.

**Example**

```bash
console#configure
console(config)#aaa ias-user username client-1
console(config-ias-user)#password client123
console(config-ias-user)#no password
```

The following is an example of adding a MAB Client to the IAS user database with MAC address f81f.3ccc.b157. Be sure to enter the password in upper case letters or authentication will fail with an “MD5 Validation Failure” as the password hash does not match.

```bash
console#configure
console(config)#aaa ias-user username f81f3ccc.b157
console(config-ias-user)#password F81F3CCC.B157
console(config-ias-user)#exit
console(config)#
```
password (User Exec)

Use the `password` command in User Exec mode to allow a currently logged in user to change the user password without having read/write privileges. This command should be used after the password has aged. The user is prompted to enter the old password and the new password. The special characters allowed in the password include: ! # $ % & ’ ( ) * + , . / ; < = > @ [ \ ] ^ _ ` { | } ~. User names can contain blanks if the name is surrounded by double quotes.

⚠️ **NOTE:** For commands that configure password properties, see Password Management Commands.

**Syntax**

`password`  

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

User Exec mode

**User Guidelines**

This command configures the password for a switch administrative user.

**Example**

The following example shows the prompt sequence for executing the `password` command.

```
console>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

**show aaa ias-users**

Use the `show aaa ias-users` command to display configured IAS users and their attributes. Passwords configured are not shown in the `show` command output.
**Syntax**
show aaa ias-users

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
IAS users are distinct from switch administrative users. IAS users are allowed access to network resources.

**Example**
```
console#show aaa ias-users

UserName
-------------------
Client-1
Client-2
```

**show aaa statistics**
Use the `show aaa statistics` command to display accounting statistics.

**Syntax**
show aaa statistics

**Default Configuration**
This command has no default setting.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**
This command has no user guidelines.

**Examples**

```console
console#show aaa statistics
```

Number of Accounting Notifications sent at beginning of an Exec session: 0
Errors when sending Accounting Notifications beginning of an Exec session: 0
Number of Accounting Notifications sent at end of an Exec session: 0
Errors when sending Accounting Notifications at end of an Exec session: 0
Number of Accounting Notifications sent at beginning of a command execution: 0
Errors when sending Accounting Notifications at beginning of a command execution: 0
Number of Accounting Notifications sent at end of a command execution: 0
Errors when sending Accounting Notifications at end of a command execution: 0

**show accounting methods**

Use the `show accounting methods` command to display the configured accounting method lists.

**Syntax**

```
show accounting methods
```

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

```console
console#show accounting methods
```

<table>
<thead>
<tr>
<th>AcctType</th>
<th>MethodName</th>
<th>MethodType</th>
<th>Method1</th>
<th>Method2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec</td>
<td>dfltExecList</td>
<td>start-stop</td>
<td>tacacs</td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td>dfltCmdList</td>
<td>stop-only</td>
<td>tacacs</td>
<td></td>
</tr>
<tr>
<td>Dot1x</td>
<td>dfltDot1xList</td>
<td>start-stop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>EXEC Method List</td>
<td>Command Method List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console</td>
<td>none</td>
<td>Telnet</td>
<td>none</td>
<td>SSH</td>
</tr>
</tbody>
</table>

**Command History**
Example updated in the 6.4 release.

**show accounting update**
Use this command to show the configuration of accounting updates.

**Syntax**
show accounting update

**Default Configuration**
There is no default configuration for this command.

**Command Modes**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**

```
console#show accounting update

aaa accounting update newinfo : Disabled
aaa accounting update periodic : 5 minutes
```

**Command History**
Introduced in the 6.5.2 release.
show authentication

Use this command to list the authentication methods configured on the interface and display if the Tiered Authentication feature is enabled.

Syntax

show authentication [interface {interface-id | all}]

- interface-id—The physical interface.
- all—All interfaces.

Default Configuration

There is no default configuration for this command.

Command Modes

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

console# show authentication

Tiered Authentication......................... Enabled

console# show authentication interface gi1/0/1
Port........................................... Gi1/0/1
Authentication Restart timer............... 300
Configured method order..................... dot1x mab captive-portal
Enabled method order....................... dot1x mab undefined
Configured method priority.................. undefined undefined
Enabled method priority..................... undefined undefined
Number of authenticated clients........... 1
Logical Interface............................ 0
client mac addr............................. 00:00:00:00:00:01
Authenticated Method....................... dot1x
Auth State.................................... success
Auth Status.................................. Authenticated
show authentication authentication-history

Use this command to display the authentication history on one or more interfaces.

Syntax

show authentication authentication-history {interface-id | all}
  •  interface-id—Any physical interface.

Default Configuration

There is no default configuration for this command.

Command Modes

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

crrole#show authentication authentication-history gi1/0/1

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Interface</th>
<th>MAC-Address</th>
<th>Auth Status</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 21 1919 15:06:15</td>
<td>Gi1/0/1</td>
<td>00:00:00:00:00:01</td>
<td>Authorized</td>
<td>802.1x</td>
</tr>
</tbody>
</table>

show authentication methods

Use the show authentication methods command to display information about the authentication methods.

Syntax

show authentication methods
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the authentication configuration.

```
console#show authentication methods

Login Authentication Method Lists  
---------------------------------
defaultList         : none
networkList         : local

Enable Authentication Method Lists  
----------------------------------
enableList          : enable   none
enableNetList       : enable

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableNetList
SSH      networkList          enableNetList
HTTPS       :local
HTTP        :local
DOT1X       :
```

**show authentication statistics**
Use this command to display the Authentication Manager statistics on one or more interfaces.
**Syntax**

`show authentication statistics interface-id`

- `interface-id`—The physical interface.

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
config# show authentication statistics gi1/0/1

Port........................................... Gi1/0/1
802.1x attempts................................ 1
802.1x failed attempts......................... 0
Mab attempts................................... 0
Mab failed attempts............................ 0
Captive-portal attempts....................... 0
Captive-Portal failed attempts.............. 0
```

**show authorization methods**

Use the `show authorization methods` command to display the configured authorization method lists.

**Syntax**

`show authorization methods`

**Default Configuration**

This command has no default setting.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
Command authorization is supported only for the line, telnet, and SSH access methods.

**Example**
```
console#show authorization methods

Exec Authorization List         Methods
-----------------------------------------------
dfltExecAuthList                none

Command Authorization List      Methods
-----------------------------------------------
dfltCmdAuthList                 none

Line       Exec Method Lists      Command Method Lists
----------  ---------------------  ---------------------
Console    dfltExecAuthList       dfltCmdAuthList
Telnet     dfltExecAuthList       dfltCmdAuthList
SSH        dfltExecAuthList       dfltCmdAuthList

Network Authorization  Methods
---------------------- -------
Dot1x                  radius
```

**show users accounts**
Use the `show users accounts` command to display the local user status with respect to user account lockout and password aging.

**Syntax**
```
show users accounts
```

**Default Configuration**
This command has no default configuration.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

User accounts are distinct from the IAS user accounts. IAS users are allowed access to network resources when authenticating via AAA. User accounts are switch administrators allowed access to the switch administrator console. The following fields are displayed by this command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td>Local user account’s user name.</td>
</tr>
<tr>
<td>Privilege</td>
<td>User’s access level (read only-1 or read/write-15). Use level 0 to block a user’s access.</td>
</tr>
<tr>
<td>Password Aging</td>
<td>Indicates whether password aging is enabled and the password aging period.</td>
</tr>
<tr>
<td>Password Expiry Date</td>
<td>Current password expiration date in date format.</td>
</tr>
<tr>
<td>Lockout</td>
<td>Displays the user’s lockout status (True or False).</td>
</tr>
</tbody>
</table>

**Example**

The following example displays information about the local user database.

```
console(config)#show users accounts
```

<table>
<thead>
<tr>
<th>UserName</th>
<th>Privilege</th>
<th>Password Aging</th>
<th>Password Expiry date</th>
<th>Lockout</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>15</td>
<td>200</td>
<td>Jan 13 1915 00:32:12</td>
<td>False</td>
</tr>
</tbody>
</table>

**show users login-history**

Use the show users login-history command in Global Configuration mode to display information about the login history of users.
Syntax

show users login-history [username|long]

- username — name of user. (Range: 1-64 characters)
- long — display only the user login name

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command displays switch administrative user information.

Example

The following example shows user login history outputs.

```
console#show users login-history
Login Time            Username  Protocol  Location
--------------------  --------- ---------  -----------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:29:29  Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

Command History

Syntax updated in 6.4 release.

username

Use the **username** command in Global Configuration mode to add a new user to the local user (switch administrator) database. The default privilege level is 1. The command optionally allows the specification of an Administrative Profile for a local user.

Use the **no** form of this command to remove the username from the local user database.
Syntax

username name {nopassword|password} password

no username name

- name—The name of the user. Range: 1-64 printable characters. The special characters allowed in the username include ! # $ % & ‘ ( ) * + , - . / : ; < = > @ [ \ ] ^ _ ` { | } ~. Question marks are disallowed. User names can contain blanks if the name is surrounded by double quotes.

- password—The authentication password for the user. Range: 8-64 characters. This value can be 0 [zero] if the no passwords min-length command has been executed. The special characters allowed in the password include ! # $ % & ‘ ( ) * + , - . / : ; < = > @ [ \ ] ^ _ ` { | } ~. Question marks are disallowed.

- level—The user’s privilege level. Level 0 can be assigned by a level 15 user to another user to restrict that user’s access to configuration commands. Supported access levels are 0, 1, or 15. Enter access level 0 to restrict the user’s access, 1 for Read Access, or 15 for Read/Write Access.

- nopassword—Configure a switch administrator with no password. Note that the SSH is configured to require a password to access the switch. Use of a password for administrative access is highly recommended.

- profile—The name of the administrative profile(s) to apply to this user. An administrative profile is mutually exclusive with a privilege level.

- encrypted—Encrypted password entered, copied from another switch configuration. Password strength checking is not applied to the encrypted string.

Default Configuration

The default privilege level is 1.

Command Mode

Global Configuration mode

User Guidelines

The following rules and restrictions apply:
- User accounts have an associated privilege level, a user name, and a user password.
- The password is saved internally in hashed format and never appears in clear text anywhere in the UI.
- An administrator (privilege level 15) may create additional administrator accounts.
- An administrator may delete any or all administrator accounts, including his own.

To use the ! character as part of the username or password string, it should be enclosed within quotation marks. For example, username “test!xyz” password “test!xyz” includes an exclamation point in both the username and password.

Up to 8 users may be created. If the password strength feature is enabled, it checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. If the encrypted keyword is entered, no password strength checking is performed as the password is encrypted and the system does not have the capability of decrypting the password. Privilege level 0 is restricted from using Privileged Exec or any Configuration level commands. There is effectively no difference between Privilege level 1 and 15.

The following table lists the completion messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion Message</td>
<td>No message is displayed.</td>
</tr>
<tr>
<td>Error Completion Message</td>
<td>Could not set user password!</td>
</tr>
</tbody>
</table>
### Example

The following example configures user `bob` with password `xxxyymmmm` and user level 15.

```
console(config)# username bob password ?
<password> Enter the password. The special characters allowed in the password include `~` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `_` `-` `=` `[` `]` `|` `\` `:` `;` `'` `<` `>` `.` `/,`. 

console(config)# username bob password xxxyymmmm privilege 15
```

### username unlock

Use the `username unlock` command in Global Configuration mode to unlock a locked user account. Only a user with read/write access can reactivate a locked user account.

### Syntax

```
username username unlock
```
**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command applies to switch administrator accounts.
Privilege level 0 is restricted from using Privileged Exec or any Configuration-level commands. There is effectively no difference between privilege level 1 and 15.
Administrative Profiles Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The administrative profiles capability provides the network administrator control over which commands a user (switch administrator) is allowed to execute. The administrator is able to group commands into a “profile” and assign a profile to a user upon authentication. This provides more granularity than simply allowing read-only and read-write users. It may be, for example, that a particular user is only allowed to manage the Captive Portal feature but not allowed to manage any other of the switch features.

This capability is similar to the industry standard “User Roles” feature. The main difference is that the Administrative Profile is obtained via authentication rather than via authorization. This was necessary because Dell EMC Networking does not support AAA authorization of users.

Functionally, the Administrative Profiles feature allows the network administrator to define a list of rules which control the commands which may be executed by a user. These rules are collected in a “profile.” A rule defines a set of commands to which a user is permitted or denied access. Alternatively, a rule may define a CLI command mode to which the user is permitted or denied access. The rule numbers determine the order in which the rules are applied: Rules are applied in descending numerical order until there is a match. Rules may use regular expressions for command matching. All profiles have an implicit “deny all” rule such that any command which does not match any rules in the profile is considered to have been denied by that profile.

It is possible to assign a user more than one profile. If there are conflicting rules in profiles, the “permit” rule always takes precedence over the “deny” rule, i.e., if any profile assigned to a user permits a command, then the user is permitted access to that command. A user may be assigned up to 16 profiles. A number of profiles are provided by default. These profiles may not be altered by the switch administrator.

If the successful authentication method does not provide an Administrative Profile for a user, then the user is permitted access based upon the user’s privilege level (as in previous releases). This means that if a user successfully
passes enable authentication, the user is permitted access to all commands. This is also true if none of the Administrative Profiles provided are configured on the switch.

**RADIUS and TACACS+**

The network administrator may configure a custom attribute to be provided by the server during authentication. The RADIUS and TACACS+ applications process this custom attribute and provide this data to the User Manager for configuring the user profile.

The custom attribute is defined as:

```
cisco-av-pair=shell:roles="roleA roleB ..."
```

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-profile</td>
<td>show admin-profiles</td>
</tr>
<tr>
<td>description (Administrative Profile Configuration)</td>
<td>show admin-profiles brief</td>
</tr>
<tr>
<td>rule</td>
<td>show cli modes</td>
</tr>
</tbody>
</table>

**admin-profile**

Use the `admin-profile` command in Global Configuration mode to create an administrative profile. The system-defined administrative profiles cannot be deleted. When creating a profile, the user is placed into Administrative Profile Configuration mode.

Use the `no` form of the command to delete an administrative profile and all its rules.

**Syntax**

```
admin-profile profile-name
no admin-profile profile-name
```

- profile-name—The name of the profile to create or delete. Range: 1 to 16 alphanumerics characters – may also include a hyphen.
**Default Configuration**
The administrative profiles are defined by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
```
console(config)#admin-profile qos
console(admin-profile)#
```

**description (Administrative Profile Configuration)**
Use the `description` command in Administrative Profile Configuration mode to add a description to an administrative profile.
Use the `no` form of this command to delete the description.

**Syntax**
```
description text
no description
```
- `text`—A description of, or comment about, the administrative profile. To include white space, enclose the description in quotes. Range: 1 to 128 printable characters.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Administrative Profile Configuration mode

**User Guidelines**
The description string is required to be enclosed in quotes if it contains embedded white space. Question marks are disallowed.
Example

```
console(admin-profile)#description "This profile allows access to QoS commands."
```

**rule**

Use the `rule` command to add a rule to an administrative profile.

Use the no form of this command to delete a rule.

**Syntax**

```
rule number {deny|permit} {command command-string|mode mode-name}
no rule number
```

- number—The sequence number of the rule. Rules are applied from the highest sequence number to the lowest. Range: 1 to 256.
- command-string—Specifies which commands to permit or deny. The command-string may contain spaces and regular expressions. The command string is required to be enclosed in quotes if it contains embedded white space. Range: 1 to 128 characters. Regular expressions should conform to Henry Spencer’s implementation of the POSIX 1003.2 specification.

**NOTE:** Note: In this usage, the beginning and end of line meta-characters have no meaning.

- mode-name—The name of the CLI mode to which the profile will permit or deny access.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Administrative Profile Configuration mode

**User Guidelines**

This command has no user guidelines.
Example

console(admin-profile)#rule 1 permit command "access-list *"
console(admin-profile)#

show admin-profiles

Use the show admin-profiles command to show the administrative profiles. If the optional profile name parameter is used, only that profile will be shown.

Syntax

show admin-profiles [name profile-name]

- profile-name—The name of the administrative profile to display.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following admin profiles are predefined and may not be deleted or changed by the administrator:

- Profile: network-admin
- Profile: network-security
- Profile: router-admin
- Profile: multicast-admin
- Profile: dhcp-admin
- Profile: CP-admin
- Profile: network-operator.

Example

console#show admin-profiles name qos

Profile: qos
Description: This profile allows access to QoS commands.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Perm</th>
<th>Type</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>permit</td>
<td>command</td>
<td>access-list *</td>
</tr>
<tr>
<td>2</td>
<td>permit</td>
<td>command</td>
<td>access-group *</td>
</tr>
<tr>
<td>3</td>
<td>permit</td>
<td>mode</td>
<td>class-map</td>
</tr>
</tbody>
</table>

**show admin-profiles brief**

Use the `show admin-profiles brief` command to list the names of the administrative profiles defined on the switch.

**Syntax**

`show admin-profiles brief`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show admin-profiles brief

Profile: network-admin
Profile: network-security
Profile: router-admin
Profile: multicast-admin
Profile: dhcp-admin
Profile: CP-admin
Profile: network-operator
```
**show cli modes**

Use the `show cli modes` command to list the names of all the CLI modes.

**Syntax**

`show cli modes`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

These are the generic mode names to be used in the `rule` command above. These are not the same as the prompt which is displayed in a particular mode.

**Example**

```
console#show cli modes

user-exec
privileged-exec
global-config
ethernet-config
port-channel-config
```
E-mail Alerting Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

E-mail Alerting is an extension of the logging system. The Dell EMC Networking logging system allows the user to configure a variety of destinations for log messages. This feature adds e-mail configuration capabilities, by which the log messages are sent to a configured SMTP server such that an operator may receive the log in an e-mail account of their choice.

Figure 1: Log Messages Severity Level

The network operator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination e-mail addresses. Log messages in the urgent group are sent immediately to SMTP server with each log message in a separate mail. Log messages in the non-urgent group are batched into a single e-mail message and after a configurable delay.

Only the minimum part (MUA functionality of RFC 4409) required by the switch or router to send the messages to the SMTP server is supported. Some SMTP servers insist on authentication before the messages may be received by them. The minimum part (MUA functionality of RFC 4954) required by the switch or router to become authenticated by the SMTP server is supported. Only plain text authentication is supported.

Commands in this Section

This section explains the following commands:
**logging email**

Use the **logging email** command in Global Configuration mode to enable e-mail alerting and set the lowest severity level for which log messages are e-mailed. Use the **no** form of the command to disable e-mail alerting.

**Syntax**

logging email [severity]

no logging email

- severity—If you specify a severity level, log messages at or above the severity level are e-mailed. The severity level may either be specified by keyword or as an integer from 0 to 7. The accepted keywords, and the numeric severity level each represents, are as follows.
  - emergency (0)
  - alert (1)
  - critical (2)
  - error (3)
  - warning (4)
  - notice (5)
  - info (6)
  - debug (7)
**Default Configuration**

E-mail alerting is disabled by default. When e-mail alerting is enabled, log messages at or above severity Warning are e-mailed.

**Command Mode**

Global Configuration mode

**User Guidelines**

The `logging email` command with no arguments enables e-mail alerting. Specify a severity to set the severity level of log messages that are e-mailed in a non-urgent manner. Log messages at or above this severity level, but below the urgent severity level, are collected together until the log time expires (the time specified in the `logging email logtime` command) and then e-mailed in a single e-mail message. If you set the non-urgent severity level to the same value as the urgent severity level, then no log messages are e-mailed non-urgently. See the `logging email urgent` command to specify the urgent severity level. The command `no logging email` disables all e-mail alerting.

**logging email urgent**

Use the `logging email urgent` command in Global Configuration mode to set the lowest severity level at which log messages are e-mailed in an urgent manner. To revert the urgent severity level to its default value, use the `no` form of this command.

**Syntax**

logging email urgent {severity | none}

no logging email urgent

- severity—If you specify a severity level, log messages at or above the severity level are e-mailed. The severity level may either be specified by keyword or as an integer from 0 to 7. The accepted keywords, and the numeric severity level each represents, are as follows.
  - emergency (0)
  - alert (1)
  - critical (2)
– error (3)
– warning (4)
– notice (5)
– info (6)
– debug (7)

• none—If you specify this keyword, no log messages are e-mailed urgently. All log messages at or above the non-urgent level (configured with the logging email command) are e-mailed in batch.

Default Configuration
The default severity level is alert.

Command Mode
Global Configuration mode

User Guidelines
Log messages at or above this severity level are considered urgent. By default, Emergency and Alert log messages are considered urgent. Urgent log messages are e-mailed immediately, one log message per e-mail message, and do not wait for the log time to expire. Urgent log messages are not e-mailed unless you enable e-mail alerting with the logging email command.

logging email message-type to-addr
Use the logging email message-type to-addr command in Global Configuration mode to configure the To address field of the e-mail. The message types supported are urgent, non-urgent, and both. For each supported severity level, multiple e-mail addresses can be configured. For example, for urgent type of messages, there could be multiple addresses configured.

Syntax
logging email message-type {urgent | non-urgent | both} to-addr to-email-addr
no logging email to-addr to-addr message-type
no logging email message-type {urgent | non-urgent | both} to-addr to-email-addr

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration

**User Guidelines**
The to-email-addr is the address to which the email is sent.
Urgent | non-urgent | both—The priority with which the email is queued. Urgent email is sent immediately. Non-urgent email is queued and sent periodically.

**Example**
```
console(config)#logging email message-type urgent to-addr admin123@dell.com
```

**Command History**
Example added in the 6.4 release.

**logging email from-addr**
Use the `logging email from-addr` command in Global Configuration mode to configure the From address of the e-mail. Use the `no` form of this command to remove the e-mail source address.

**Syntax**
```
logging email from-addr from-email-addr
no logging email from-addr
```

**Default Configuration**
This command has no default configuration.
**Command Mode**
Global Configuration

**User Guidelines**
The from-addr in this command is the email address of the email sender. Many mail servers will validate the from address of an email to ensure that abuse of the email server does not occur.

**Example**
console(config)#logging email from-addr dell@gmail.com

**Command History**
Example added in the 6.4 release.

**logging email message-type subject**
Use the `logging email message-type subject` command in Global Configuration mode to configures subject of the e-mail. Use the `no` form of this command to remove the existing subject and return to the default subject.

**Syntax**
logging email message-type message-type subject subject
no logging email message-type message-type subject

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration

**User Guidelines**
The user must enter the message-type parameter manually as tab and space bar completion do not work for this parameter.
**Example**

```console
console(config)#logging email message-type urgent subject UrgentLog
```

**Command History**

Example added in the 6.4 release.

**logging email logtime**

Use the `logging email logtime` command in Global Configuration mode to configure the value of how frequently the queued messages are sent.

**Syntax**

```plaintext
logging email logtime time duration
no logging email logtime
```

- `time duration`—Time in minutes. Range: 30 – 1440.

**Default Configuration**

The default value is 30 minutes.

**Command Mode**

Global Configuration

**User Guidelines**

This command has no user guidelines.

**Example**

```console
console(config)#logging email logtime 50
```

**Command History**

Example added in the 6.4 release.
logging email test message-type

Use the logging email test message-type command in Global Configuration mode to test whether or not an e-mail is being sent to an SMTP server.

Syntax

logging email test message-type message-type message-body message-body

- message-type—Urgent, non-urgent, or both
- message-body—The message to log. Enclose the message in double quotes if it contains any spaces.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

Example

crash(config)#logging email test message-type urgent message-body urgentlog

Command History

Example added in the 6.4 release.

show logging email statistics

Use the show logging email statistics command to show the statistics about the e-mails. The command displays information on how many e-mails are sent, how many e-mails failed, how long it has been since the last e-mail was sent.

Syntax

show logging email statistics
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec

**User Guidelines**
This command has no user guidelines.

**Example**
```
console#show logging email statistics

No of email Failures so far.................... 0
No of email sent so far......................... 0
Time since last email Sent.................... 00 days 00 hours 00 mins 00 secs
```

**clear logging email statistics**
Use the `clear logging email statistics` command to clear the e-mail alerting statistics.

**Syntax**
clear logging email statistics

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec

**User Guidelines**
This command has no user guidelines.

**Example**
```
console#clear logging email statistics
```
Command History
Example added in the 6.4 release.

security

Use the security command in Mail Server Configuration mode to set the e-mail alerting security protocol. This enables and disables the switch to use TLS authentication with the SMTP Server. If the administrator sets the TLS mode and, if the SMTP sever does not support TLS mode, then no e-mail goes to the SMTP server.

Syntax
security {tlsv1 | none}

Default Configuration
The default value is disabled.

Command Mode
Mail Server Configuration

User Guidelines
This command has no user guidelines.

Example
console(config)#mail-server 10.131.1.11
console(mail-server)#security tlsv1

Command History
Example added in the 6.4 release.

mail-server ip-address | hostname

Use the mail-server ip-address | hostname command in Global Configuration mode to configure the SMTP server IP address and change the mode to Mail Server Configuration mode. Use the no form of this command to remove the configured SMTP server address.
Syntax

mail-server {ip-address | hostname}
no mail-server {ip-address | hostname}

• ip-address—An IPv4 or IPv6 address.
• hostname—The DNS name of an SMTP server.

Default Configuration

The default configuration for a mail server is shown in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Alert Mail Server Port</td>
<td>25</td>
</tr>
<tr>
<td>Email Alert Security Protocol</td>
<td>none</td>
</tr>
<tr>
<td>Email Alert Username</td>
<td>admin</td>
</tr>
<tr>
<td>Email Alert Password</td>
<td>admin</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

User Guidelines

The server address can be in the IPv4, IPv6, or DNS FQDN name format.

port (Mail Server Configuration Mode)

Use the **port** command in Mail Server Configuration mode to configure the TCP port to use for communication with the SMTP server. The default for no security is 25 (SMTP). The port for TLSv1 is port 465. The range is 1025 to 65535. Use the **no** form of the command to revert the SMTP port to the default port.

Syntax

port port
no port
**Default Configuration**
The default value is 25 (SMTP).

**Command Mode**
Mail Server Configuration

**User Guidelines**
Port 25 is the standard SMTP port for cleartext messages. Port 465 is the standard port for messages sent using TLSv1.

**Example**
```
console(config)#mail-server 10.131.1.11
console(mail-server)#port 1024
```

**Command History**
Example added in the 6.4 release.
Description updated in the 6.4 release.

**username (Mail Server Configuration Mode)**
Use the `username` command in Mail Server Configuration mode to configure the username required by the authentication. Use the `no` form of the command to revert the username to the default value.

**Syntax**
```
username username
no username
```

**Default Configuration**
The default value for username is `admin`.

**Command Mode**
Mail Server Configuration
User Guidelines
This command has no user guidelines.

Example
console(config)#mail-server 10.131.1.11
console(mail-server)#username admin

Command History
Example added in the 6.4 release.

password (Mail Server Configuration Mode)
Use the password command in Mail Server Configuration mode to configure the password required to authenticate to the e-mail server. Use the no form of the command to revert the password to the default value.

Syntax
password password
no password

Default Configuration
The default value for password is admin.

Command Mode
Mail Server Configuration

User Guidelines
This command has no user guidelines.

Example
console(config)#mail-server 10.131.1.11
console(mail-server)#password admin123

Command History
Example added in the 6.4 release.
**show mail-server**

Use the `show mail-server` command to display the configuration of all the mail servers or a particular mail server.

**Syntax**

```
show mail-server {ip-address | hostname | all}
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show mail-server all
Mail Servers Configuration:

No of mail servers configured......................1

  Email Alert Mail Server Address.................. 10.131.1.11
  Email Alert Mail Server Port...................... 465
  Email Alert SecurityProtocol...................... tls
  Email Alert Username.............................. admin
  Email Alert Password.............................. password

console#show mail-server all
Mail Servers Configuration:

No of mail servers configured......................1

  Email Alert Mail Server Address.................. 10.131.1.11
  Email Alert Mail Server Port...................... 465
  Email Alert SecurityProtocol...................... tls
  Email Alert Username.............................. admin
  Email Alert Password.............................. password

console#show mail-server 10.131.1.11
```
Email Alert Mail Server Address................. 10.131.1.11
Email Alert Mail Server Port....................... 465
Email Alert Security Protocol....................... tlsv1
Email Alert Username.............................. admin
Email Alert Password.............................. password

**Command History**

Example added in the 6.4 release.
RADIUS Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Authentication of users in a large network can be significantly simplified by making use of a single database of accessible information supplied by an Authentication Server. These servers commonly use the Remote Authentication Dial In User Service (RADIUS) protocol as defined by RFC 2865.

RADIUS permits access to a user’s authentication and configuration information contained on the server only when requests are received from a client that shares an encrypted secret with the server. This secret is never transmitted over the network in an attempt to maintain a secure environment. Any requests from clients that are not appropriately configured with the secret or access from unauthorized devices are silently discarded by the server.

RADIUS conforms to a client/server model with secure communications using UDP as a transport protocol. It is extremely flexible, supporting a variety of methods to authenticate and statistically track users. It is very extensible allowing for new methods of authentication to be added without disrupting existing network functionality.

Dell EMC Networking supports a RADIUS client in conformance with RFC 2865 and accounting functions in conformance with RFC2866 and RFC6911 for attribute 168. The RADIUS client will apply user policies under control of the RADIUS server, e.g. password lockout or login time of day restrictions. The RADIUS client supports up to 32 named authentication and accounting servers.

For the N1100-ON and N1500 Series switches, the number of supported authentication and accounting servers is 8.

RADIUS-based Dynamic VLAN Assignment

If a VLAN assignment is enabled in the RADIUS server, then as part of the response message, the RADIUS server sends the VLAN ID that the client is requested to use in the 802.1x tunnel attributes. If dynamic VLAN creation is enabled on the switch (dot1x dynamic-vlan enable) and the RADIUS
assigned VLAN does not exist on the supplicant connected interface, the assigned VLAN is dynamically created. See the `aaa authorization network default radius` command for further information. This implies that the client can connect from any port and be assigned to the appropriate VLAN, which may be already configured on an uplink interface. This gives flexibility for clients to move around the network without requiring the operator to perform additional provisioning for each network interface. Dynamic VLAN assignment uses the following RADIUS attributes from the received Access-Accept:

IETF 64 (Tunnel Type)—Set this to VLAN.
IETF 65 (Tunnel Medium Type)—Set this to 802.
IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID or VLAN name.

**RADIUS Change of Authorization**

Dell EMC Networking supports the Change of Authorization Disconnect-Request per RFC 3575. The Dell EMC Networking switch listens for the Disconnect-Request on UDP port 3799. The Disconnect-Request identifies the user session to be terminated using the following attributes:

- User-Name (IETF attribute #1)
- Acct-Session-Id (IETF attribute #44)
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

The following messages from RFC 3575 are supported:

- 40 - Disconnect-Request
- 41 - Disconnect-ACK
- 42 - Disconnect-NAK

A CoA Disconnect-Request terminates the session without disabling the switch port. Instead, CoA Disconnect-Request termination causes re-initialization of the authenticator state machine for the specified host. MAC-based port control can be enabled for 802.1x sessions. In this case, if the RADIUS server issues a disconnect request and subsequently does not authorize the MAC address to access network resources, the host is effectively denied network access.
If the session cannot be located, the device returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message. The attributes returned within a CoA ACK can vary based on the CoA Request.

The administrator can configure whether all or any of the session attributes are used to identify a client session. If all is configured, all session identification attributes included in the CoA Disconnect-Request must match a session or the device returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

Dell EMC Networking supports the following attributes in responses:
- User-Name (IETF attribute #1)
- State (IETF attribute #24)
- Calling-Station-ID (IETF attribute #31)
- Acct-Session-ID (IETF attribute #44)
- Message-Authenticator (IETF attribute #80)
- Error-Cause (IETF attribute #101)

A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

The Dell EMC Networking switch starts listening to the client again based on reauthentication timer.

Refer to the RADIUS Change of Authorization section in the Users Configuration Guide for examples of configuring RADIUS CoA.

**Commands in this Section**

This section explains the following commands:

| acct-port | primary | radius server source-ip |
acct-port

Use the acct-port command to set the port on which the RADIUS accounting server listens for connections. Use the no form of this command to reset the port to the default.

**Syntax**

acct-port port

no acct-port

• port — The layer 4 port number of the accounting server (Range: 1 - 65535).

**Default Configuration**

The default value of the port number is 1813.

**Command Mode**

RADIUS Server Accounting mode


**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example sets port number 56 for accounting requests.

```
console(config)#radius server acct 3.2.3.2
console(Config-acct-radius)#acct-port 56
```

**attribute 6**

Use the `attribute 6` command to configure processing of the RADIUS Service-Type attribute.

**Syntax**

```
attribute 6 [on-for-login-auth|mandatory]
no attribute 6 [on-for-login-auth|mandatory]
```

**Default Configuration**

By default, the Service-Type is not included in the Access-Request message sent to the authentication server.

**Command Mode**

RADIUS Server Configuration

**User Guidelines**

- **on-for-login**—If the `on-for-login` parameter is enabled, the Service-Type TLV is send in the Access-Request message.

- **mandatory**—If the mandatory parameter is enabled, the Service-Type attribute is required and validated in the Access-Accept packet received from the RADIUS server. Dell EMC Networking N-Series switches accept the Login-User (1) and Administrative-User (6) values in the Access-Accept message returned from the RADIUS server. If the mandatory parameter is not configured, the Service-Type TLV received in an Access-Accept packet is ignored.
Command History
Introduced in version 6.3.0.1 firmware. Updated in 6.3.5.0 firmware.

Example
This example configures the switch to send the Service-Type attribute to the RADIUS server in the Access-Request message.

```
console#conf
console(config)#radius server auth 4.3.2.1
console(config-auth-radius)#attribute 6 on-for-login-auth
```

This example configures the switch to process and validate the Service-Type received in the Access-Accept message from the RADIUS server.

```
console#conf
console(config)#radius server auth 4.3.2.1
console(config-auth-radius)#attribute 6 mandatory
```

attribute 8
Use the attribute 8 command to configure the switch to send the RADIUS Framed-IP-Address attribute in the Access-Request message sent to a specific RADIUS authentication server. The switch sends the IP address of the host attempting to authenticate in the Framed-IP-Address attribute in the Access-Request sent to the authentication server.

Syntax
attribute 8 include-in-access-req
no attribute 8 include-in-access-req

Default Configuration
By default, the Framed-IP-Address is not included in the Access-Request message sent to the authentication server.

Command Mode
RADIUS Server Configuration

User Guidelines
There are no user guidelines for this command.
**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#conf
console(config)#radius server auth 4.3.2.1
console(config-auth-radius)#attribute 8 include-in-access-req
```

**attribute 25**

Use the `attribute 25` command to enable the switch to send the RADIUS Class attribute as supplied by the RADIUS server in accounting messages sent to the specific accounting server.

**Syntax**

```
attribute 25 include-in-access-req
no attribute 25 include-in-access-req
```

**Default Configuration**

By default, the Class attribute is included in the accounting messages sent to the accounting server if received in the Access-Accept from the RADIUS authentication server.

**Command Mode**

RADIUS Server Configuration

**User Guidelines**

The switch sends the Class attribute value supplied by the RADIUS server in the Access-Accept message if enabled. If disabled, the Class attribute received from the RADIUS server is ignored. The Class attribute may be up to 16 octets in length

**Command History**

Introduced in version 6.3.0.1 firmware.
Example
console#conf
calendar(config)#radius server auth 4.3.2.1
calendar(config-auth-radius)#attribute 25 include-in-access-req

attribute 31
Use the attribute 31 command to alter the format of the MAC address sent to the RADIUS server in the Calling-Station-Id attribute when authenticating using either 802.1X MAC-based or MAB authentication for an interface. Use the no form of the command to return the MAC address format to the default.

Syntax
attribute 31 mac format { ietf | unformatted | legacy } [lower-case | upper-case]
no attribute 31 mac format

- ietf—Format the MAC address as 18-DB-F2-25-B2-D4. The default is upper case.
- unformatted—Format the MAC address as 18dbf225b2d4. The default is lower case.
- legacy—Format the MAC address as 18:db:f2:25:b2:d4. The default is lower case.
- lower-case—Format hexadecimal characters using the character set [0-9a-f].
- upper-case—Format hexadecimal characters using the character set [0-9A-F].

Default Configuration
The default is to send the Calling-Station-ID in upper case unformatted format.

Command Mode
RADIUS Server Configuration
**User Guidelines**

Use this command to override the format of the Calling-Station-ID MAC address sent in authentication Access-Request for ports configured for 802.1X MAC-based or MAB authentication for a specific RADIUS server.

This command is only supported for 802.1X authentication.

This command overrides the global configuration for attribute 31 (Calling-Station-ID). Use the mab request format command to control the formatting of the User-Name (1) attribute.

**Command History**

Introduced in version 6.3.0.1 firmware. Description update in release 6.5.0 to remove the User-Name formatting control.

**Example**

This example configures the format of the MAC address sent in MAC based authentication to IETF lower case for the RADIUS server at address 1.2.3.4. MAB must be configured on the switch in an active authentication list, IEEE 802.1X must be configured, and a RADIUS server must also be configured.

```console
console(config)#radius server auth 1.2.3.4
console(config-auth-radius)# attribute 31 mac format ietf lower-case
```

**attribute 168 include-in-access-req**

Use the `attribute 168 include-in-access-req` command to enable the switch to send the RADIUS Framed-IPv6-Address attribute in Access-Request messages sent to the RADIUS authentication server.

**Syntax**

- `attribute 168 include-in-access-req`
- `no attribute 168 include-in-access-req`

**Default Configuration**

By default, RADIUS attribute 168 is not sent.
**Command Mode**

RADIUS Server Configuration mode.

**User Guidelines**

The switch sends the IPv6 address of the host attempting to access the network in the Framed-IPv6-Address attribute if it is available to the switch. If accounting is enabled and the address is available to the switch, the switch will send the IPv6 address in the Access-Request, Acct-Start/Acct-Interim/Acct-Stop messages sent to the accounting server.

The switch discovers the client IPv6 address via its inclusion in the RADIUS Access-Accept, or via DHCPv6 snooping. DHCPv6 snooping must be enabled for the switch to discover a host IPv6 address via DHCPv6.

After an Access-Accept has been received by the switch and the switch grants the host access to the network, it may take a few seconds before the DHCPv6 transaction completes. Use the `aaa accounting delay-start` command to delay the sending of the Acct-Start packet to the accounting server.

Use the `show dot1x clients` command to display the RADIUS server supplied IPv6 address, if any.

RADIUS attribute 168 Framed-IPv6-Address is defined in RFC 6911.

**Command History**

Command introduced in firmware release 6.5.2.

**authentication event fail retry**

Use the `authentication event fail retry` command to select the number of times authentication is reattempted by the user for an IEEE 802.1X supplicant. Use the `no` form of the command to return the number of maximum attempts to the default value.

**Syntax**

`authentication event fail retry max-attempts`

`no authentication event fail retry`
max-attempts — The number of times RADIUS authentication is allowed to fail before failing the authentication and moving to the next authentication method. Default 1. Range 1–5.

Default Configuration
By default, the number of failed authentication attempts is 1. An authentication failure is declared failed after a single authentication attempt.

Command Mode
Interface Configuration mode, Interface Range mode

User Guidelines
This command is only applicable to IEEE 802.1X authentication with a RADIUS server. It has no effect on any other authentication method.

This parameter is independent of, and does not control, the number of times the authenticator will attempt to contact the RADIUS servers. For example, if the max-retries for a single configured RADIUS server is set to 3 and the max-attempts is set to 2, on a supplicant login attempt, the authenticator will send up to three access requests to the RADIUS server before returning failure. The authenticator will then re-invoke supplicant authentication method which allows the RADIUS back end to again send up to three requests to the RADIUS server before the authenticator allows IEEE 802.1x to stop supplicant authentication and to invoke the quiet period for the supplicant.

This command sets the limit for retring failed authentications for RADIUS. The switch attempts authentication based on the selected method and if authentication returns an error (as opposed to a failure), the next authentication method is attempted regardless of this setting.

For example, if one or multiple RADIUS servers are configured and no RADIUS server responds to the authentication message, RADIUS returns an error and the next authentication method is attempted even when the retry parameter is configured to a value larger than 1.

Example
The following example configures the switch to allow IEEE 802.1X supplicants to fail authentication (e.g., enter incorrect passwords) three times before invoking the quiet timer on the interface.
console#conf
console(config)#authentication enable
console(config)#interface gi1/0/3
console(config-if-Gi1/0/3)#authentication order dot1x
console(config-if-Gi1/0/3)#authentication event fail retry 3

**Command History**
Introduced in version 6.3.0.1 firmware.

**auth-port**
Use the **auth-port** command in RADIUS Server Configuration mode to set the port number on which the RADIUS server listens for authentication requests.

**Syntax**

```
auth-port auth-port-number
```

- **auth-port-number** — Port number for authentication requests. (Range: 1 - 65535)

**Default Configuration**
The default value of the port number is 1812.

**Command Mode**
RADIUS Server Configuration mode

**User Guidelines**
User must enter the mode corresponding to a specific RADIUS Server Configuration before executing this command.

**Example**
The following example sets the port number 2412 for authentication requests.

```
console(config)#radius server auth 192.143.120.123
cosntle(config-auth-radius)#auth-port 2412
```
automate-tester

Use the `automate-tester` command to configure liveness checking. Use the `no` form of the command to disable liveness checking.

Syntax

`automate-tester username user-name [idle-time minutes]`

`no automate-tester username`

- `username user-name`—Configure the user name to use to test the RADIUS server for liveness. The user-name should not be configured on the RADIUS server.
- `idle-time minutes`—Configure the idle time (in minutes) after which the server is quarantined and sending of test packets commences. The range is 1 to 35791 minutes.

Default Configuration

There is no default user name.
The default idle time is 60 minutes.

Command Mode

RADIUS Authentication Server Configuration mode
RADIUS Accounting Server Configuration mode

User Guidelines

RADIUS servers configured with a test username and a non-zero deadtime are tested periodically for liveness. Liveness of a server is determined by sending an Access-Request to the server using a configurable dummy login. If an Access-Reject is returned, the server is marked alive and is available for use for authentication. The radius deadtime configured retries and timeouts are applied. It is suggested that the configured values be the same as the normal RADIUS values. If a RADIUS server fails to respond, it is marked dead. Setting the deadtime to 0 disables liveness checks and configures the switch to never mark the server dead.
Configuring the user-name parameter as a valid login on the RADIUS server will induce state on the server as the server will wait for further packets from the switch. The switch will not send any further RADIUS packets to remove the state from the RADIUS server. Therefore, Dell EMC strongly recommends that the user name not be configured on the RADIUS server.

The user-name parameter accepts any printable character. Enclose the parameter in double quotes to configure embedded blanks in the user name. Successive invocations of the automate-tester command overwrite the previous values.

**Command History**

Command introduced in version 6.5 firmware.

**Example**

The following example configures an IPv4 RADIUS accounting server with the following characteristics:

Server IP address—192.168.10.1

Login—DummyLogin

Idle Time—30 minutes

**deadtime**

Use the `deadtime` command in RADIUS Server Configuration mode to configure the minimum amount of time to wait before attempting to recontact an unresponsive RADIUS server.

**Syntax**

deadtime deadtime

- `deadtime` — The amount of time that the unavailable server is skipped over. (Range: 0-2000 minutes)

**Default Configuration**

The default deadtime interval is 0 minutes, that is, the server will never be marked dead.
**Command Mode**
RADIUS Server Configuration mode

**User Guidelines**
If only one RADIUS server is configured, it is recommended to use a deadtime interval of 0.

Setting the deadtime to 0 indicates to the switch that the server should never be marked dead. This effectively disables features such as critical Voice VLAN.

If a RADIUS server is currently active and responsive, that server will be used until it no longer responds. RADIUS servers whose deadtime interval has not expired are skipped when searching for a new RADIUS server to contact.

**Example**
The following example specifies a deadtime interval of 60 minutes.
```
console(config)#radius server auth 192.143.120.123
console(config-auth-radius)#deadtime 60
```

**key**
Use the `key` command to specify the encryption key which is shared with the RADIUS server. Use the `no` form of this command to remove the key.

**Syntax**
```
key [ 0|7] key-string
no key
```
- 0—The key string that follows is the unencrypted shared secret. The length is 1–128 characters.
- 7—The key string that follows is the encrypted shared secret. The length is exactly 256 characters.
- key-string — The key string in encrypted or unencrypted form. In encrypted form, it must be 256 characters in length. In unencrypted form, it may be up to 128 characters in length.
Default Configuration
There is no key configured by default.

Command Mode
RADIUS Server Configuration mode

User Guidelines
There are no user guidelines for this command.
In an Access-Request, encrypted passwords are sent using the RSA Message Digest algorithm (MD5).
If no encryption parameter (7) is present, the key string is interpreted as an unencrypted shared secret.
Keys are always displayed in their encrypted form in the running configuration.
The encryption algorithm is the same across switches. Encrypted passwords may be copied from one switch and pasted into another switch.

Command History
Updated in version 6.3.0.1 firmware.

Example
The following two examples globally configure the RADIUS server key for all configured servers. The two examples are identical in effect.

```
console(config)#radius server auth 1.2.3.4
console(config-auth-radius)#key "This is a key string"
console(config-auth-radius)#key 0 "This is a key string"
```

msgauth
Use the msgauth command to enable the message authenticator attribute to be used for the RADIUS Authenticating server being configured. Use the “no” form of this command to disable the message authenticator attribute.

Syntax
msgauth
no msgauth

Default Configuration
The message authenticator attribute is enabled by default.

Command Mode
RADIUS Server Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(Config-auth-radius)#msgauth

name (RADIUS Server)
Use the name command to assign a list name to a RADIUS server. Use the no form of the command to return the name to the default (unspecified). The no form of the command does not require the user to enter the configured name.

Syntax
name servername
no name

- servername—The name of the server list for a RADIUS server (Range: 1 to 32 characters).

Default Configuration
The default RADIUS server list name is Default-RADIUS-Server.

Command Mode
RADIUS Server Configuration mode
**User Guidelines**

Assigning a name to multiple RADIUS authentication servers associates the servers into a list. Server lists may be used to control which authentication servers are prioritized for traffic. Names assigned to accounting servers are ignored.

Names may consist of alphanumeric characters and the underscore, dash and blanks. Embed the name in double quotes to use a name with blanks.

**NOTE:** When multiple RADIUS servers are configured with different list names, e.g. ServerName is name1 and address is 1.1.1.1 ServerName is name2 and address is 1.1.1.2 the RADIUS request is always sent to the first lexicographically ordered server list, i.e. communication with the name1 server list is attempted before moving on to the name2 server list. Even if the priority value of servers in the name2 list is lower (lower value indicates higher priority) the request is sent to the name1 servers. If no servers respond in the name1 list, the request is sent to the second name list in lexicographic order, et. seq.

A server list may consist of multiple primary server and multiple secondary servers. Within a server list, communication the primary servers is attempted first in priority order. From the multiple secondary servers, the server with the lowest priority value is tried after the primary fails. For a server list where all priorities are equal, communication is attempted based on the server name lexicographic order. For example, if name9, name1, name6 are configured in a server list, communication is attempted in the order name1, then name6, then name9.

Use the `show aaa servers name` command to display the server lists.

**Example**

```bash
console(config)#radius server 44.44.44.44
console(config-auth-radius)#name NAME
console(config-auth-radius)#no name
```

**primary**

Use the `primary` command to specify that a configured server should be the primary server in a server list. Multiple primary servers can be configured for each group of servers which have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of the specified name, it uses the primary server that has the specified server name
by default. If it fails to communicate with the primary server for any reason, it uses the backup servers configured with the same server name. These backup servers are identified as the “Secondary” type.

**Syntax**

`primary`

**Default Configuration**

There is no primary authentication server by default.

**Command Mode**

RADIUS Server Configuration mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(Config-auth-radius)#primary
```

**priority**

Use the `priority` command in RADIUS Server Configuration mode to specify the order in which the servers are to be used, with 0 being the highest priority.

**Syntax**

`priority priority`

- `priority` — Sets server priority level. (Range 0-65535)

**Default Configuration**

The default priority is 0.

**Command Mode**

RADIUS Server Configuration mode
User Guidelines
User must enter the mode corresponding to a specific RADIUS server before executing this command.

Example
The following example specifies a priority of 10 for the designated server.

```
console(config)#radius server auth 192.143.120.123
console(config-auth-radius)#priority 10
```

radius server attribute 4
Use the `radius server attribute 4` command to set the network access server (NAS) IPv4 address for the RADIUS server. The NAS-IP-Address is RADIUS attribute number 4. Use the `no` version of the command to set the value to the default.

Syntax

```
radius server attribute 4 ip-address
no radius server attribute 4
```

- ip-address — Specifies the IPv4 address to be used as the RADIUS attribute 4, the NAS-IP-Address.

Default Configuration
If a RADIUS server has been configured on the switch, the default NAS-IP-Address sent to the RADIUS server is the address of the switch or the address of the interface over which the Access-Request is sent.

Command Mode
Global Configuration mode

User Guidelines
This command does not alter the address in the IP header in Access-Requests transmitted to the RADIUS server. It only configures the NAS-IP-Address attribute sent to the RADIUS server inside the RADIUS Access-Request packet. This capability is useful when configuring multiple RADIUS clients.
(switches) to simulate a single RADIUS client for scalability. The RADIUS Acct-Session-Id may overlap if multiple switches are configured with the same NAS-IP-Address.

The configured NAS-IP-Address need not be the same as the IPv4 source address transmitted in the IP header. Use the `radius server source-ip` command to configure the IPv4 source address transmitted in the IP header.

**Example**

The following example sets the NAS IP address RADIUS attribute 4 to 192.168.10.22.

```
console(config)#radius server attribute 4 192.168.10.22
```

**radius server attribute 6**

Use the `radius server attribute 6` command to configure the use of the RADIUS Service-Type attribute.

**Syntax**

```
radius server attribute 6 {on-for-login-auth|mandatory}
no radius server attribute 6 {on-for-login-auth|mandatory}
```

**Default Configuration**

By default, the switch does not send the Service-Type attribute to the RADIUS server in the Access-Request packets. By default, the switch ignores the Service-Type received in Access-Accept packets.

**Command Mode**

Global Configuration

**User Guidelines**

`on-for-login`—This parameter globally configures the switch to send the RADIUS Service-Type attribute in the Access-Request message sent to all RADIUS authentication servers. The switch sends the Service-Type value Administrative (6) for administrators attempting to access the switch console and sends Service-Type value Login (1) for users attempting to access the network.
mandatory—This parameter enables processing and validation of the Service-Type parameter received from the RADIUS server in Access-Accept messages. Dell EMC Networking N-Series switches accept the Login-User (1) or Administrative-User (6) values in the Access-Accept message returned from the RADIUS server. Access-Accept messages without one of those values are treated as if an Access-Reject message has been received.

**Command History**
Introduced in version 6.3.0.1 firmware. Updated in 6.3.0.5 firmware.

**Example**
This command configures the switch to send the Service-Type attribute in the Access-Request message sent to the RADIUS server.

```
console#conf
console(config)#radius server attribute 6 on-for-login-auth
```

**radius server attribute 8**
Use the `radius server attribute 8 include-in-access-req` command to enable the switch to send the RADIUS Framed-IP-Address attribute in Access-Request messages sent to the authentication server.

**Syntax**
```
radius server attribute 8 include-in-access-req
no radius server attribute 8 include-in-access-req
```

**Default Configuration**
By default, RADIUS attribute 8 is not sent.

**Command Mode**
Global Configuration

**User Guidelines**
If accounting is enabled and the address is available to the switch, the switch will send the IPv4 address in the Access-Request, Acct-Start/Acct-Interim/Acct-Stop messages sent to the RADIUS server.
The switch discovers the client IPv4 address via its inclusion in the RADIUS Access-Accept, via DHCPv4 snooping. DHCPv4 snooping must be enabled for the switch to discover a host IPv4 prefix via DHCP.

After an Access-Accept has been received by the switch and the switch grants the host access to the network, it may take a few seconds before the DHCP transaction completes. Use the **aaa accounting delay-start** command to delay the sending of the Acct-Start packet to the accounting server. Accounting packets are not sent for ports placed in the Guest VLAN. Multiple hosts are allowed access on a port configured in auto mode which is placed in the Guest VLAN.

Use the **show dot1x clients** command to display the RADIUS discovered IPv4 address, if any.

**Command History**

Introduced in version 6.3.0.1 firmware. Command updated in firmware release 6.5.2.

**Example**

```console
console#conf
console(config)#radius server attribute 8 include-in-access-req
```

**radius server attribute 25**

Use the **radius server attribute 25** command to globally enable the switch to send the RADIUS Class attribute as supplied by the RADIUS server in accounting messages sent to the accounting server.

**Syntax**

```
radius server attribute 25 include-in-access-req
no radius server attribute 25 include-in-access-req
```

**Default Configuration**

By default, the switch sends the Class attribute to the accounting server if received in the Access-Accept from the RADIUS authentication server.
Command Mode
Global Configuration

User Guidelines
The switch sends the Class attribute value supplied by the RADIUS server in the RADIUS Access-Accept message if enabled. If disabled, the Class attribute received in the RADIUS Access-Accept message is ignored. The Class attribute may be up to 16 octets in length.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console#conf
console(config)#radius server attribute 25 include-in-access-req

radius server attribute 31
Use the radius server attribute 31 command to alter the format of the MAC address sent to the RADIUS server when authenticating using 802.1X authentication. Use the no form of the command to return the MAC address format to the default.

Syntax
radius server attribute 31 mac format { ietf | unformatted | legacy } [lower-case | upper-case]
no radius server attribute 31 mac format
  • ietf—Format the MAC address as 18-DB-F2-25-B2-D4. The default is upper case.
  • unformatted—Format the MAC address as 18dbf225b2d4. The default is lower case.
  • legacy—Format the MAC address as 18:db:f2:25:b2:d4. The default is lower case.
  • lower-case—Format hexadecimal characters using the character set [0-9a-f].
• **upper-case**—Format hexadecimal characters using the character set [0-9A-F].

**Default Configuration**

By default, the switch sends the Calling-Station-Id MAC address in unformatted uppercase format.

**Command Mode**

Global Configuration

**User Guidelines**

Use this command to override the format of MAC addresses sent in the Calling-Station-Id (attribute 31) for Access-Requests for ports configured for MAC based 802.1x authentication or MAB.

This command is only supported for 802.1X authentication.

This command does not override the per RADIUS server configuration for attribute 31. Use the **mab request format** command to configure formatting the User-Name attribute.

**Command History**

Introduced in version 6.3.0.1 firmware. Updated in release 6.5.0 to remove formatting of the User-Name attribute.

**Example**

This example globally configures the format of the MAC address sent in the Calling-Station-Id attribute when using MAC based authentication to IETF lower case. It also configures interface Gi1/0/1 to use MAB. MAB must be configured on the switch in an active authentication list, IEEE 802.1X must be configured, and a RADIUS server must also be configured.

```console
console(config)#radius server attribute 31 mac format ietf lower-case
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#dot1x port-control mac-based
console(config-if-Gi1/0/1)#mab
```
radius server attribute 168

Use the `radius server attribute 168 include-in-access-req` command to enable the switch to send the RADIUS Framed-IPv6-Address attribute in Access-Request messages sent to the RADIUS authentication server.

Syntax

```
radius server attribute 168 include-in-access-req
no radius server attribute 168 include-in-access-req
```

Default Configuration

By default, RADIUS attribute 168 is not sent.

Command Mode

Global Configuration mode.

User Guidelines

The switch sends the IPv6 address of the host attempting to access the network in the Framed-IPv6-Address attribute if it is available to the switch. If accounting is enabled and the address is available to the switch, the switch will send the IPv6 address in the Access-Request, Acct-Start/Acct-Interim/Acct-Stop messages sent to the accounting server.

The switch discovers the client IPv6 address via its inclusion in the RADIUS Access-Accept, or via DHCPv6 snooping. DHCPv6 snooping must be enabled for the switch to discover a host IPv6 address.

After an Access-Accept has been received by the switch and the switch grants the host access to the network, it may take a few seconds before the DHCPv6 transaction completes. Use the `aaa accounting delay-start` command to delay the sending of the Acct-Start packet to the accounting server. Accounting messages are not sent for hosts placed in the Guest VLAN.

Use the `show dot1x clients` command to display the RADIUS Server supplied IPv6 address, if any.

RADIUS attribute 168 Framed-IPv6-Address is defined in RFC 6911.
**Command History**
Command introduced in firmware release 6.5.2.

**radius server deadtime**
Use the `radius server deadtime` command to configure the minimum amount of time to wait before attempting to recontact an unresponsive RADIUS server. To set the deadtime to 0, use the `no` form of this command.

**Syntax**

```
radius server deadtime deadtime
no radius server deadtime
```

- `deadtime` — Length of time in minutes, for which a RADIUS server is skipped over by transaction requests. (Range: 0–2000 minutes). **Deadtime** is used to mark an unavailable RADIUS server as dead until this user-configured time expires. **Deadtime** is configurable on a RADIUS server basis.

**Default Configuration**
The default dead time is 0 minutes.

**Command Mode**
Global Configuration mode

**User Guidelines**
If only one RADIUS server is configured, it is recommended that the deadtime interval be left at 0. Setting the deadtime to 0 will cause the switch to always send a RADIUS request to the RADIUS server if the server is selected. If a RADIUS server is currently active and responsive, that server will be used until it no longer responds. RADIUS servers whose deadtime interval has not expired are skipped when searching for a new RADIUS server to contact.
Example
The following example sets the minimum interval for a RADIUS server will not be contacted after becoming unresponsive.

```
console(config)#radius server deadtime 10
```

radius server
Use the radius server command to specify a RADIUS server, and enter RADIUS Server Configuration mode. To delete the specified RADIUS server, use the no form of this command.

Syntax
radius server [acct | auth] {ip–address | hostname}
no radius server {ip–address | hostname}

- acct | auth—The type of server (accounting or authentication).
- ip–address—The RADIUS server host IP address.
- hostname —Host name of the RADIUS server host. (Range: 1–255 characters).

Default Configuration
The default server type is authentication. The default server name is Default-RADIUS-Server. The default port number is 1812 for an authentication server and 1813 for an accounting server.

Command Mode
Global Configuration mode

User Guidelines
RADIUS servers are keyed by the host name/IP address, therefore it is advisable to use unique server host names. Use the show aaa servers {accounting | authentication} command to display the hostname/IP address to list name mapping.

Multiple authentication servers may be configured with the same name using the name command.
Dell EMC Networking implements a two-level hierarchy for RADIUS servers. The top level is a list of servers which is alphabetically ordered by name. Each server within the top level may be associated with the multiple server hostnames/IP addresses. When multiple RADIUS servers are configured with different names (for example, one server is name1 with address 1.1.1.1 and the second server is name2 with address 1.1.1.2):

- The RADIUS request is always sent to the first server in the alphabetically ordered list of servers, for example, server name1 is attempted before moving on to the server name2 server. Even if the priority value of hosts/IP addresses in server name2 is lower (a lower value indicates a higher priority), the request would be sent to server name1. If, for the server name1, all the configured hostnames/IP addresses fail to respond, the request is sent to the second configured server.

- Within a server, the primary server is always tried first. Use the `primary` command in RADIUS Server configuration mode to designate a primary server. One can have multiple secondary hostnames/IP addresses in the same server list. From the multiple secondary hostnames/IP addresses, the one with the lowest priority value is tried first. In a server with multiple hostnames/IP addresses with the same priority, the order of attempts is based on lexicographic order. For example, if hostnames name9, name1, name6 are configured as secondary hosts, the hostnames are attempted in the order name1, name6, name9 when the primary host fails to respond.

**Command History**
Updated syntax in version 6.5 firmware.

**Example**
The following example specifies a RADIUS authentication server with the following characteristics:

- Server IP address — 192.168.10.1
- Server Name — name1
- Type — primary

```
console(config)#radius server 192.168.10.1
console(config-auth-radius)#name name1
console(config-auth-radius)#primary
```
The following shows an example configuration with two servers (list1 and list2), each of which has a Primary and Secondary IP addresses:

```
console(config)#show aaa servers authentication

*  Host Address  Server Name  Port  Type
-----  ------------  -------  ------ -------
  1.2.3.1  list1  1812    Primary
  4.3.2.2  list2  1812    Secondary
  4.3.2.1  list2  1812    Primary
  1.2.3.5  list1  1812    Secondary
  1.2.3.4  list1  1812    Secondary

* currently selected server
```

**radius server key**

Use the `radius server key` command to set the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. Use the `no` form of the command to disable the key.

**Syntax**

```
radius server key [ 0 | 7 ]key-string
no radius server key
```

- **0**—The key string that follows is the unencrypted shared secret. The length is 1–128 characters.
- **7**—The key string that follows is the encrypted shared secret. The length is exactly 256 characters.
- **key-string** — The key string in encrypted or unencrypted form. In encrypted form, it must be 256 characters in length. In unencrypted form, it may be up to 128 characters in length.

**Default Configuration**

The default is an empty string.

**Command Mode**

Global Configuration
**User Guidelines**

In an Access-Request, encrypted passwords are sent using the RSA Message Digest algorithm (MD5).

If no encryption parameter (7) is present, the key string is interpreted as an unencrypted shared secret.

Keys are always displayed in their encrypted form in the running configuration.

The encryption algorithm is the same across switches. Encrypted passwords may be copied from one switch and pasted into another switch configuration.

**Command History**

Updated in version 6.3.0.1 firmware.

**Example**

The following two examples globally configure the RADIUS server key for all configured servers. The two examples are identical in effect.

```
console(config)#radius server key "This is a key string"
console(config)#radius server key 0 "This is a key string"
```

**radius server retransmit**

Use the `radius server retransmit` command to specify the number of times the RADIUS client will retransmit requests to the RADIUS server. To reset the default configuration, use the `no` form of this command.

**Syntax**

radius server retransmit retries

no radius server retransmit

- retries — Specifies the retransmit value. (Range: 1–10)

**Default Configuration**

The default is 1 retry.

**Command Mode**

Global Configuration mode
User Guidelines
This command has no user guidelines.

Example
The following example configures the number of times the RADIUS client attempts to retransmit requests to the RADIUS server to five attempts.
console(config)#radius server retransmit 5

radius server source-ip
Use the radius server source-ip command to specify the source IPv4 address used in the IP header for communication with RADIUS servers. To return to the default, use the no form of this command. 0.0.0.0 is interpreted as a request to use the IPv4 address of the outgoing IP interface.

Syntax
radius server source-ip source
no radius server source-ip
• source — Specifies the source IPv4 address.

Default Configuration
The default IPv4 address is the outgoing interface IPv4 address.

Command Mode
Global Configuration mode

User Guidelines
The command configures the source IP address present in the IPv4 header. It is not the optional NAS-IP-Address in the RADIUS message. Use the radius server attribute 4 command to configure the NAS-IP-Address attribute sent in the RADIUS Access-Request message.

Example
The following example configures the source IP address used for communication with RADIUS servers to 10.1.1.1.
radius server source-interface

Use the `radius server source-interface` command to select the interface from which to use the IP address in the source IP address field of transmitted RADIUS packets. Use the `no` form of the command to revert to the default IP address.

**Syntax**

```
radius server source-interface {loopback loopback-id | vlan vlan-id}
no radius server source-interface
```

- `loopback-id` — A loopback interface identifier.
- `vlan-id` — A VLAN identifier.

**Default Configuration**

By default, the switch uses the assigned switch IP address as the source IP address for RADIUS packets. This is either the IP address assigned to the VLAN from which the RADIUS packet originates or the out-of-band interface IP address.

**Command Mode**

Global Configuration

**User Guidelines**

The source IP address of RADIUS packets sent to a server should match the NAS IP address configured on the RADIUS server. A mismatch may lead to a RADIUS packet timeout.

Loopback interfaces are not supported on the Dell EMC N1100-ON Series switches.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#conf
```
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#radius server source-interface vlan 1

radius server timeout

Use the radius server timeout command in Global Configuration mode to set the interval for which a switch waits for a server to reply. To restore the default, use the no form of this command.

**Syntax**

radius server timeout timeout

no radius server timeout

- timeout — Specifies the timeout value in seconds. (Range: 1–30)

**Default Configuration**

The default value is 15 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the interval for which a switch waits for a server to reply to 5 seconds.

console(config)#radius server timeout 5

radius server vsa send authentication

Use the radius server vsa send authentication command to enable the switch to process vendor-specific attributes during authentication.
Syntax
radius server vsa send authentication
no radius server vsa send authentication

Default Configuration
By default, VSA Attribute 26, Vendor ID 9, and Vendor type 9 are not processed by the switch.

Command Mode
Global Configuration mode

User Guidelines
This command does not affect processing of any VSA’s other than VSA 26, Vendor ID 9, Vendor type 9, Sub-type 1. It does not affect processing of Voice VLAN or Admin/Login.

Predefined ACL Selection using VSA Attribute 26
This method selects an ACL that is already configured on the switch. The extended-access-control-list-name is the name of an existing ACL pre-configured on the switch. The ACL need not be statically pre-configured on the port prior to RADIUS configuring the ACL on the port prior to authorizing the port (it would be removed in any case as statically configured ACLs on a port are removed prior to configuring a dynamic ACL).

ip:inacl={ extended-access-control-list-name }
ipv6:inacl={ extended-access-control-list-name }

- The ip token indicates an IPv4 ACL name follows the equals sign.
- The IPv6 token indicates an IPv6 ACL name follows the equals sign.
- The extended-access-control-list-name token identifies an IP/IPv6 Extended ACL Name of an existing ACL. The name is case sensitive.
- The tokens ip:inacl and ipv6:inacl are in lower case and are followed by an equals sign with no intervening white space.

Different authentication sessions, as in the case of the data and voice VLAN authenticating independently, may both have Dynamic ACLs. It is recommended that the DACLs be carefully designed so that they work in
harmony, such as, at a minimum, no ACL numbers are duplicated across the DACLs. DACLs are applied at the port level and are capable of affecting any traffic ingressing the port.

**Predefined ACL Examples**

- `ip:inacl=Named_ACL`
- `ipv6:inacl=Named_IPv6_ACL`

**Dynamic ACL Definition**

This method uses ACL syntax to create a new ingress ACL on the switch:

- `ip:inacl[#number]={extended-access-control-list}`
- `ipv6:inacl[#number]={ extended-access-control-list}`

- The ip token indicates an IPv4 ACL definition follows the equals sign.
- The ipv6 token indicates an IPv6 ACL definition follows the equals sign.
- #number is the ACL sequence number in decimal format. Range 1–2147483647.
- The tokens ip:inacl and ipv6:inacl are in lower case and are followed by an equals sign with no intervening white space.
- extended-access-control-list means an extended IPv4/IPv6 Extended ACL CLI rule definition beginning with the `{permit|deny}` tokens followed by the protocol `{every | eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-55}` for IPv4 and `{ every icmpv6| ipv6 | sctp | tcp | udp}` for IPv6.

**Dynamic ACL Example (Extended syntax, that is, ip access-list extended ...)**

- `ip:inacl#100=permit ip any 209.165.0.0 0.0.255.255`
- `ip:inacl#110=permit ip any 209.166.0.0 0.0.255.255`
- `ip:inacl#120=permit ip any 209.167.0.0 0.0.255.255`

Multiple ip:inacl /ipv6:inacl av-pairs may be present in the RADIUS message. However, only the first definition will be applied for the authentication session. Different sessions, as in the case of the data and voice VLAN authenticating independently, may both have Dynamic ACLs. It is recommended that the DACLs be carefully designed so that they work in harmony, such as, at a minimum, no ACL numbers are duplicated across the DACLs. DACLs are applied at the port level and are capable of affecting any traffic ingressing the port. If there are syntax errors in the received ACLs (other than duplicate rules), the ACL rules are not applied, the RADIUS Access-Accept is treated as an Access-Reject, and a WARN log message or
"Interface X/X/X not authorized. Application of downloaded ACL did not complete due to invalid syntax XXXXX" is issued indicating that a received RADIUS rule is misconfigured with invalid syntax or configured with both ip:traffic-class and inacl rules and identifying the affected interface. If Accounting is enabled, the Acct-Start packet is not sent. An EAP-Failure is sent to the 802.1X client.

Command History
Command introduced in firmware version 6.5.2.

retransmit
Use the retransmit command in RADIUS Server Configuration mode to specify the number of times the RADIUS client retransmits requests to the RADIUS server.

Syntax
retransmit retries
  • retries — Specifies the retransmit value. (Range: 1-10 attempts)

Default Configuration
The default number for attempts is 3.

Command Mode
RADIUS mode

User Guidelines
User must enter the mode corresponding to a specific RADIUS server before executing this command.

Example
The following example of the retransmit command specifies five retries.

```
console(config)#radius server 192.143.120.123
console(config-auth-radius)#retransmit 5
```
show aaa servers

Use the show aaa servers command to display the list of configured RADIUS servers and the values configured for the global parameters of the RADIUS servers.

Syntax

show aaa servers [accounting | authentication] [name [servername]]

- accounting—This optional parameter will cause accounting servers to be displayed.
- authentication—This optional parameter will cause authentication servers to be displayed.
- name—This optional parameter will cause the server names to be displayed instead of the server configuration parameters.
- servername—Will cause only the server(s) with server-name name to be displayed. There are no global parameters displayed when this parameter is specified.

Default Configuration

All authentication servers are displayed by default.

Command Mode

User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Authentication Servers</td>
<td>The number of RADIUS Authentication servers that have been configured.</td>
</tr>
<tr>
<td>Configured Accounting Servers</td>
<td>The number of RADIUS accounting servers that have been configured.</td>
</tr>
<tr>
<td>Named Authentication Server Groups</td>
<td>The number of configured named authentication RADIUS server groups.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Named Accounting Server Groups</td>
<td>The number of configured named accounting RADIUS server groups.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The configured timeout value, in seconds, for request retransmissions.</td>
</tr>
<tr>
<td>Retransmit</td>
<td>The configured value of the maximum number of times a request packet is retransmitted.</td>
</tr>
<tr>
<td>Dead Time</td>
<td>The configured length of time an unavailable RADIUS server is skipped.</td>
</tr>
<tr>
<td>RADIUS Accounting Mode</td>
<td>A global parameter to indicate whether the accounting mode for all the servers is enabled or not.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Mode</td>
<td>A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Value</td>
<td>A global parameter that specifies the IP address to be used in NAS-IP-Address attribute to be used in RADIUS requests.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>The source interface from which the source IP address is obtained.</td>
</tr>
<tr>
<td>RADIUS Attribute 6</td>
<td>A global parameter that specifies if the Service-Type is sent to the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Attribute 8</td>
<td>A global parameter that indicates if the Authenticate-Only attribute is sent to the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Attribute 25</td>
<td>A global parameter that indicates if the Class attribute is sent to the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Attribute 31</td>
<td>A global parameter that indicates if the Calling-Station-ID is sent to the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Attribute 31 format</td>
<td>A global parameter that indicates the format of the Calling-Station-ID attribute.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware. Command updated in version 6.5.2 firmware.
Example

console#show aaa servers

<table>
<thead>
<tr>
<th>IP address</th>
<th>Type</th>
<th>Port</th>
<th>TimeOut</th>
<th>Retran.</th>
<th>DeadTime</th>
<th>Source IP</th>
<th>Prio.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.130.50.107</td>
<td>Auth</td>
<td>1812</td>
<td>Global</td>
<td>Global</td>
<td>Global</td>
<td>Global</td>
<td>0</td>
</tr>
<tr>
<td>10.130.50.107</td>
<td>Acct</td>
<td>1813</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Global values

Number of Configured Authentication Servers.... 1
Number of Configured Accounting Servers........ 1
Number of Named Authentication Server Groups... 1
Number of Named Accounting Server Groups....... 1
Number of Retransmits.......................... 3
Timeout Duration............................... 15
Deadtime....................................... 0
Source IP...................................... 0.0.0.0
Source Interface............................... Default
RADIUS Accounting Mode......................... Enable
RADIUS Attribute 4 Mode ....................... Disable
RADIUS Attribute 4 Value ...................... 0.0.0.0
RADIUS Attribute 6 Mode ....................... Disable
RADIUS Attribute 8 Mode ....................... Enable
RADIUS Attribute 168 Mode ..................... Enable
RADIUS Attribute 25 Mode ..................... Enable
RADIUS Attribute 31 MAC Format Value......... Unformatted upper-case
RADIUS Accounting Interim Update.............. Enable
RADIUS Accounting delayed start Mode.......... Enable
RADIUS Accounting extended delay Value........ 60

console#show aaa servers name Default-RADIUS-Server

RADIUS server name.............................. Default-RADIUS-Server
Current Server IP Address...................... 10.130.50.107
Number of retransmits.......................... 3
Timeout duration............................... 15
Deadtime....................................... 0
RADIUS server auth-port....................... 1812
CoA port....................................... 3799
Source IP...................................... 0.0.0.0
RADIUS accounting mode....................... Enable
Secret configured.............................. Yes
show radius statistics

Use the show radius statistics command to show the statistics for an authentication or accounting server.

Syntax

show radius statistics [accounting | authentication] [{ipaddress | hostname | name servername}]

- accounting | authentication—The type of server (accounting or authentication).
- ipaddress—The RADIUS server host IP address.
- hostname—Host name of the RADIUS server host. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, console(config)#snmp-server host "host name"
- servername—The alias used to identify the server.

Default Configuration

By default, the command displays authentication server statistics.

Command Mode

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following fields are displayed for accounting servers:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Accounting Server Name</td>
<td>Name of the accounting server.</td>
</tr>
<tr>
<td>Server Host Address</td>
<td>IP address of the host.</td>
</tr>
<tr>
<td>Round Trip Time</td>
<td>The time interval, in hundredths of a second, between the most recent Accounting Response and the Accounting Request that matched it from this RADIUS accounting server.</td>
</tr>
<tr>
<td>Requests</td>
<td>The number of RADIUS Accounting Request packets sent to this server not including the retransmissions.</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>The number of RADIUS Accounting Request packets retransmitted to this RADIUS accounting server.</td>
</tr>
<tr>
<td>Responses</td>
<td>The number of RADIUS packets received on the accounting port from this server.</td>
</tr>
<tr>
<td>Malformed Responses</td>
<td>The number of malformed RADIUS Accounting Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS Accounting Response packets containing invalid authenticators received from this accounting server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Accounting Request packets destined for this server that have not yet timed out or received a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of accounting timeouts on this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of packets unknown type which were received from this server on accounting port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on accounting port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

The following fields are displayed for authentication servers:
### Security Commands

#### Example

```plaintext
console#show radius statistics accounting 192.168.37.200
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server Name</td>
<td>Name of the authenticating server.</td>
</tr>
<tr>
<td>Server Host Address</td>
<td>IP address of the host.</td>
</tr>
<tr>
<td>Access Requests</td>
<td>The number of RADIUS Access Request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Access Retransmissions</td>
<td>The number of RADIUS Access Request packets retransmitted to this RADIUS authentication server.</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>The number of RADIUS Access Accept packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>The number of RADIUS Access Reject packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>The number of RADIUS Access Challenge packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Malformed Access Responses</td>
<td>The number of malformed RADIUS Access Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS Access Response packets containing invalid authenticators or signature attributes received from this server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Access Request packets destined for this server that have not yet timed out or received a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of authentication timeouts to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of packets unknown type which were received from this server on the authentication port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on authentication port and dropped for some other reason.</td>
</tr>
</tbody>
</table>
source-ip

Use the `source-ip` command in RADIUS Server Configuration mode to specify the source IP address to be used for communication with RADIUS servers. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

**Syntax**

```
source-ip source
```

- source — A valid source IP address.

**Default Configuration**

The IP address is of the outgoing IP interface.
**Command Mode**

RADIUS Server Configuration mode

**User Guidelines**

The administrator must enter the mode corresponding to a specific RADIUS server before executing this command.

**Example**

The following example specifies 10.240.1.23 as the source IP address.

```
console(config)#radius server host 192.143.120.123
console(config-auth-radius)#source-ip 10.240.1.23
```

**timeout**

Use the timeout command in RADIUS mode to set the timeout value in seconds for the designated RADIUS server.

**Syntax**

```
timeout timeout
```

- **timeout** — Timeout value in seconds for the specified server. (Range: 1-30 seconds.)

**Default Configuration**

The default value is 15 seconds.

**Command Mode**

RADIUS mode

**User Guidelines**

User must enter the mode corresponding to a specific RADIUS server before executing this command.

**Example**

The following example specifies the timeout setting for the designated RADIUS Server.
usage
Use the usage command in RADIUS mode to specify the usage type of the server.

Syntax
usage type
  • type — Variable can be one of the following values: login, dot1x or all.

Default Configuration
The default variable setting is all.

Command Mode
RADIUS mode

User Guidelines
User must enter the mode corresponding to a specific RADIUS server before executing this command.

Example
The following example specifies usage type login.

console(config)#radius server host 192.143.120.123
console(config-radius)#timeout 20

console(config)#radius server host 192.143.120.123
console(config-auth-radius)#usage login
TACACS+ Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

TACACS+ provides access control for networked devices via one or more centralized servers, similar to RADIUS this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

Dell EMC Networking supports authentication of a user using a TACACS+ server. When TACACS+ is configured as the authentication method for a user login type (CLI/HTTP/HTTPS), the NAS will prompt for the user login credentials and request services from the TACACS+ client; the client will then use the configured list of servers for authentication and provide results back to the NAS. The TACACS+ server list is configured with one or more hosts defined via their network IP address; each can be assigned a priority to determine the order in which the TACACS+ client will contact them, a server is contacted when a connection attempt fails or times out for a higher priority server. Each server host can be separately configured with a specific connection type, port, time-out, and shared key, or the global configuration may be used for the key and time-out. Like RADIUS, the TACACS+ server may do the authentication itself, or redirect the request to another back-end device, all sensitive information is encrypted and the shared secret is never passed over the network.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>tacacs-server host</td>
</tr>
<tr>
<td>port</td>
<td>tacacs-server key</td>
</tr>
<tr>
<td>priority</td>
<td>tacacs-server source-interface</td>
</tr>
</tbody>
</table>
key

Use the key command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon.

Syntax
key [0|7] key-string
no key

- 0—The key string that follows is the unencrypted shared secret. The length is 1–128 characters.
- 7—The key string that follows is the encrypted shared secret. The length is 256 characters.
- key-string — Specifies the key string in encrypted or unencrypted form. It may be up to 128 characters in length in unencrypted format and 256 characters in length in encrypted format.

Default Configuration
If left unspecified, the key-string parameter defaults to the global value.

Command Mode
TACACS Configuration mode

User Guidelines
The key command accepts any printable characters for the key except a question mark. Enclose the string in double quotes to include spaces within the key. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

If no encryption parameter is present, the key string is interpreted as an unencrypted shared secret.
Keys are always displayed in their encrypted form in the running configuration.

In an Access-Request, encrypted passwords are sent using the RSA Message Digest algorithm (MD5).

The encryption algorithm is the same across switches. Encrypted passwords may be copied from one switch and pasted into another switch configuration.

**Command History**

Updated in version 6.3.0.1 firmware.

**Example**

The following example sets the authentication encryption key.

```
console(config-tacacs)#key "This is a key string"
console(config-tacacs)#key 0 "This is a key string"
```

**port**

Use the `port` command in TACACS Configuration mode to specify a port number on which a TACACS server listens for connections.

**Syntax**

```
port [port-number]
```

- `port-number` — The server port number. If left unspecified, the default port number is 49. (Range: 0–65535)

**Default Configuration**

The default port number is 49.

**Command Mode**

TACACS Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example displays how to specify TACACS server port number 1200.

```
console(config-tacacs)#port 1200
```

**priority**
Use the `priority` command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority.

**Syntax**

```
priority [priority]
```

- **priority** — Specifies the priority for servers. 0 (zero) is the highest priority. (Range: 0–65535).

**Default Configuration**
If left unspecified, this parameter defaults to 0 (zero).

**Command Mode**
TACACS Configuration mode

**User Guidelines**
This command has no user guidelines.

Example
The following example shows how to specify a server priority of 10000.

```
console(config-tacacs)#priority 10000
```

**show tacacs**
Use the `show tacacs` command to display the configuration and statistics of a TACACS+ server.

**Syntax**

```
show tacacs [ip-address]
```
• ip-address — The name or IP address of the host.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

The following example displays TACACS+ server settings.

```console
console#show tacacs

Global Timeout: 5

<table>
<thead>
<tr>
<th>Server Address</th>
<th>Port</th>
<th>Timeout</th>
<th>Priority</th>
<th>Source Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.254.24.162</td>
<td>49</td>
<td>Global</td>
<td>0</td>
<td>Loopback 0</td>
</tr>
</tbody>
</table>
```

tacacs-server host

Use the `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. To delete the specified hostname or IP address, use the `no` form of this command.

**Syntax**

```
tacacs-server host {ip-address | hostname}
no tacacs-server host {ip-address | hostname}
```

- ip-address — The IP address of the TACACS+ server.
- hostname — The hostname of the TACACS+ server. (Range: 1-255 characters).
**Default Configuration**

No TACACS+ host is specified.

**Command Mode**

Global Configuration mode

**User Guidelines**

To specify multiple hosts, multiple `tacacs-server host` commands can be used. TACACS servers are keyed by the host name, therefore it is advisable to use unique host names.

**Example**

The following example specifies a TACACS+ host.

```
console(config)#tacacs-server host 172.16.1.1
console(config-tacacs)#
```

**tacacs-server key**

Use the `tacacs-server key` command in Global Configuration mode to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. To disable the key, use the `no` form of this command.

**Syntax**

```
tacacs-server key [ 0 | 7 ] [key-string]
```

**no tacacs-server key**

- **0**—The key string that follows is the unencrypted shared secret. The length is 1–128 characters.
- **7**—The key string that follows is the encrypted shared secret. The length is fixed at 256 characters.
- **key-string** — Specifies the key string in encrypted or unencrypted form. It may be up to 128 characters in length in unencrypted format and is exactly 256 characters in length in encrypted format.
**Default Configuration**

The default is an empty string.

**Command Mode**

Global Configuration mode

**User Guidelines**

The tacacs-server key command accepts any printable characters for the key except a question mark. Enclose the string in double quotes to include spaces within the key. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

If no encryption parameter is present, the key string is interpreted as an un-encrypted shared secret.

Keys are always displayed in their encrypted form in the running configuration.

In an Access-Request, encrypted passwords are sent using the RSA Message Digest algorithm (MD5).

The encryption algorithm is the same across switches. Encrypted passwords may be copied from one switch and pasted into another switch.

**Command History**

Updated in version 6.3.0.1 firmware.

**Example**

The following example sets the authentication encryption key.

```
console(config)#tacacs-server key "This is a key string"
console(config)#tacacs-server key 0 "This is a key string"
```

**tacacs-server source-interface**

Use the `tacacs-server source-interface` command to select the interface from which to use the IP address in the source IP address field of transmitted TACACS packets. Use the `no` form of the command to revert to the default IP address.
Syntax

```
tacacs-server source-interface { loopback loopback-id | vlan vlan-id }
no tacacs-server source-interface
```

- `loopback-id` — Identifies the loopback interface.
- `vlan-id` — Identifies the VLAN.

**Default Configuration**

By default, the switch uses the assigned switch IP address as the source IP address for TACACS packets. This is either the IP address assigned to the VLAN from which the TACACS packet originates or a loopback interface IP address.

**Command Mode**

Global Configuration

**User Guidelines**

The source interface must have an assigned IP address (either manually or via another method such as DHCP). Loopback interfaces are not supported on the Dell EMC N1100-ON Series switches.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#conf
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#tacacs-server source-interface vlan 1
```

**tacacs-server timeout**

Use the `tacacs-server timeout` command in Global Configuration mode to set the interval during which a switch waits for a server host to reply. To restore the default, use the `no` form of this command.
Syntax

tacacs-server timeout [timeout]
no tacacs-server timeout
  • timeout — The timeout value in seconds. (Range: 1–30)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the timeout value as 30.

console(config)#tacacs-server timeout 30

timeout

Use the timeout command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used.

Syntax

timeout [timeout]
  • timeout — The timeout value in seconds. (Range: 1–30)

Default Configuration

If left unspecified, the timeout defaults to the global value.

Command Mode

TACACS Configuration mode
**User Guidelines**
This command has no user guidelines.

**Example**
This example shows how to specify the timeout value.

```
console(config-tacacs)#timeout 23
```
Local Area Networks (LANs) are often deployed in environments that permit the attachment of unauthorized devices. The networks also permit unauthorized users to attempt to access the LAN through existing equipment. In such environments, the administrator may desire to restrict access to the services offered by the LAN.

Port-based network access control makes use of the physical characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port. Port-based network access control prevents access to the port in cases in which the authentication and authorization process fails. A port is defined as a single point of attachment to the LAN.

The Dell EMC Networking switches support an 802.1x Authenticator service with a local authentication server or authentication using remote RADIUS or TACACS servers. Refer to "AAA Commands " on page 860 for information on configuring connectivity to a RADIUS or TACACS authentication server or to configure the local authentication service.

Dell EMC Networking switches also support 802.1X accounting to RADIUS or TACACS servers. Refer to the “AAA Commands” section to configure 802.1X accounting.

MD5 or none is the supported authentication method for communication with an authentication server. Dell EMC Networking does not support encryption of switch initiated authenticator/authentication server communication. However, Dell EMC Networking switches are capable of transporting end-to-end encrypted traffic such as EAP-TLS between a supplicant and an authenticator.

**802.1x Monitor Mode**

Monitor mode is a special mode that can be enabled in conjunction with 802.1X authentication. It allows network access even in case where there is a failure to authenticate but logs the results of the authentication process for diagnostic purposes. The exact details are described in the below sections. The main aim of the monitor mode is to provide a mechanism to the operator
to be able to identify the short-comings in the configuration of a 802.1x authentication on the switch without affecting the network access to the users of the switch.

There are three important aspects to this feature after activation:

1. To allow successful authentications using the returned information from authentication server.
2. To provide a mechanism to report unsuccessful authentications without negative repercussions to the user due to operator errors or failure cases from the Authentication server or supplicants.
3. To accurately report the data received from the successful and unsuccessful operations so that the operator can make the appropriate changes or learn where the problem areas are.

The monitor mode can be configured globally on a switch. If the switch fails to authenticate the user for any reason (say RADIUS access reject from RADIUS server, RADIUS time-out, or the client itself is 802.1x unaware), the client is authenticated and is undisturbed by the failure condition(s). The reasons for failure are logged and buffered into the local logging database such that the operator can track the failure conditions. Clients authenticated when monitor mode is enabled are always assigned to the default port PVID if no VLAN is supplied from the RADIUS server, and clients are assigned to RADIUS VLAN if filter-ID is a mismatch.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x dynamic-vlan enable</td>
<td>dot1x system-auth-control</td>
<td>server-key</td>
</tr>
<tr>
<td>dot1x eapolflood</td>
<td>dot1x system-auth-control</td>
<td>show dot1x</td>
</tr>
<tr>
<td></td>
<td>monitor</td>
<td></td>
</tr>
<tr>
<td>dot1x initialize</td>
<td>dot1x timeout quiet-period</td>
<td>show dot1x authentication-history</td>
</tr>
<tr>
<td>mab</td>
<td>dot1x timeout re-authperiod</td>
<td>show dot1x clients</td>
</tr>
<tr>
<td>default mab</td>
<td>dot1x timeout server-timeout</td>
<td>show dot1x interface</td>
</tr>
</tbody>
</table>
dot1x dynamic-vlan enable

Use the **dot1x dynamic-vlan enable** command in Global Configuration mode to enable the capability of creating VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch. Use the **no** form of the command to disable this capability.

**Syntax**

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

**Default Configuration**
The default value is Disabled.

**Command Mode**
Global Configuration
**User Guidelines**

This command has no user guidelines.

**dot1x eapolflood**

This command enables the flooding of received IEEE 802.1x frames in the VLAN. Use the **no** form of the command to return the processing of EAPOL frames to the default.

**Syntax**

dot1x eapolflood

no dot1x eapolflood

**Default Configuration**

By default, the switch does not forward received IEEE 802.1x frames, even if 802.1x is not enabled on the switch. This is the default behavior required by IEEE 802.1x-2010.

**Command Mode**

Global Configuration mode

**User Guidelines**

Local processing of IEEE 802.1x frames must be disabled (**no dot1x system-auth-control**) for this capability to be enabled. This capability is useful in situations where the authenticator device is placed one or more hops away from the authenticating host. The intervening switch will flood all received IEEE 802.1x frames in the VLAN.

Flooding of IEEE 802.1x frames makes end stations vulnerable to a denial of service attack should another end station record and play back certain flooded EAPOL frames at a high rate.
**dot1x initialize**

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

**Syntax**

dot1x initialize [interface interface-id]

- interface-id—The port to be initialized.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

There are no user guidelines for this command.

**mab**

Use the `mab` command to configure the switch to enable MAC Authentication Bypass (MAB) authentication for devices connected to the interface. Use the `no` form of this command to disable MAB on an interface.

**Syntax**

mab

no mab

**Default Configuration**

MAC Authentication Bypass is disabled by default.

**Command Mode**

Interface Configuration (Ethernet) mode
**User Guidelines**

Authentication of a user via MAB will not occur until the “dot1x time-out guest-vlan-period” timer expires.

When using MAB, configure the user name attributes with the supplicant MAC address using the `mab request format` command.

**Command History**

Updated syntax in version 6.5 firmware.

**Example**

The following example sets MAC Authentication Bypass on interface gigabitethernet 1/0/2:

```bash
console(config-if-Gi1/0/2)#dot1x port-control mac-based
console(config-if-Gi1/0/2)#mab
```

**default mab**

Use the `default mab` command to configure the switch to transmit EAP or CHAP or PAP credentials to the RADIUS server for MAB-authenticated devices connected to the interface. Use the `no` form of the command to set the protocol to the default.

**Syntax**

default mab [eap|chap|pap]

no default mab

- eap—Use EAP Message Digest 5 authentication.
- pap—Use Password Authentication Protocol.

**Default Configuration**

The default protocol is EAP-MD5.

**Command Mode**

Interface Configuration (Ethernet) mode
User Guidelines

This command configures the RADIUS authentication protocol used for MAB devices connected to the interface.

CHAP and PAP are not supported for TACACS authentication.

The switch sends the following information to the RADIUS server for CHAP Access-Requests:

1–User-Name—MAC address of MAB device.
3–CHAP-Password = Encrypted User Name.
4–NAS-IP-Address—IP address of the switch.
5–NAS-Port—Our internal port number.
6–Service-Type is set to 10 (Call-Check).
12–Framed-MTU—Port/switch MTU—header length (for example, 1500).
31–Calling-Station ID—Switch MAC address.
60–CHAP-Challenge (if auth type is CHAP).
61–NAS-Port-Type (Ethernet 15).
87–NAS-Port-Id (e.g., Gigabitethernet 1/0/15)

The switch sends the following information to the RADIUS server for CHAP Access-Requests:

1–User-Name—MAC address of MAB device.
2–User-Password—MAC Address of the MAB device (encrypted).
4–NAS-IP-Address—IP address of the switch.
5–NAS-Port—Our internal port number.
6–Service—Type is set to 10 (Call-Check).
12–Framed-MTU—Port/switch MTU—header length (for example, 1500).
31–Calling-Station ID—Switch MAC address.
61–NAS-Port-Type (Ethernet 15).
87–NAS-Port-Id (e.g., Gigabitethernet 1/0/15)
The switch sends the following information to the RADIUS server for EAP Access-Requests:
1–User-Name—MAC address of device.
4–NAS-IP-Address—IP address of the switch.
5–NAS-Port—Our internal port number.
12–Framed-MTU—Port/switch MTU—header length (for example, 1500).
31–Calling-Station ID—Switch MAC address.
61–NAS-Port-Type (Ethernet 15).

The Calling Station ID is formatted per the attribute 31 command.
The User-Name attribute is formatted per the attribute 1 command.
The Access-Request attribute is formatted for PAP authentication.

**Command History**
Command introduced in version 6.5 firmware.

**mab request format**
Use the *mab request format* command to configure the format of the MAC address sent in the User-Name attribute. Use the *no* form of the command to return the configuration to the default.

**Syntax**

```
mab request format attribute 1 groupsize {1 | 2 | 4 | 12} separator { - | : | . }
[lowercase | uppercase]
```

```
no mab request format attribute 1
```

- **groupsize**—The number of digits in a group.
- **separator**—The separator between groups of digits.
- **uppercase**—Use uppercase formatting for the digits.
- **lowercase**—Use lowercase formatting for the digits.
**Default Configuration**

The default format is a group size of 2, a colon separator and upper case characters, for example, 18:DB:F2:25:B2:D4.

**Command Mode**

Global Configuration mode

**User Guidelines**

A MAC address consists of 12 hexadecimal digits. The MAC address of the authentication station is sent in the User-Name attribute in a RADIUS Access-Request for MAC Authentication Bypass configured stations.

The following table shows some example formats:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Group Size</th>
<th>Separator</th>
<th>Case</th>
<th>Formatted Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>18DBF225B2D4</td>
<td>1</td>
<td>.</td>
<td>Lower</td>
<td>1.8.d.b.f.2.5.b.2.d.4</td>
</tr>
<tr>
<td>18DBF225B2D4</td>
<td>4</td>
<td>-</td>
<td>Upper</td>
<td>18DB-F225-B2D4</td>
</tr>
</tbody>
</table>

**Command History**

Command introduced in version 6.5 firmware.

**dot1x max-reauth-req**

Use the `dot1x max-reauth-req` command in Interface Configuration mode to set the maximum number of times that the switch sends Extensible Authentication Protocol EAP-Request/Identity frames to which no response is received before restarting the authentication process. To return to the default setting, use the `no` form of the command.

**Syntax**

```
dot1x max-reauth-req count
no dot1x max-reauth-req
```

- `count` — Number of times that the switch sends an EAP-Request/Identity frame before restarting the authentication process. (Range: 1–20)
**Default Configuration**

The default value for the count parameter is 2.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

This command limits the number of EAP Request/Identity messages. Use the `dot1x max-req` command to limit the number of EAP Request messages other than EAP Request/Identity.

**Command History**

Command introduced in version 6.5 firmware.

**dot1x max-req**

Use the `dot1x max-req` command to set the maximum number of times that the switch sends an Extensible Authentication Protocol EAP-Request frame to which no response is received, before restarting the authentication process. To return to the default setting, use the `no` form of this command.

**Syntax**

```
  dot1x max-req count
  no dot1x max-req
```

- `count` — Number of times that the switch sends an EAP-Request/Identity frame before restarting the authentication process. (Range: 1–10)

**Default Configuration**

The default value for the count parameter is 2.

**Command Mode**

Interface Configuration (Ethernet) mode
User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

This command limits the number of EAP-Requests other than EAP Request/Identity. Use the `dot1x max-reauth-req` command to limit the number of EAP Request/Identity messages.

Example

The following example sets the number of times that the switch sends an EAP-request/identity frame to 6.

```
console(config)# interface gigabitethernet 1/0/16
console(config-if-Gi1/0/16)# dot1x max-req 6
```

dot1x max-users

Use the `dot1x max-users` command in Interface Configuration mode to set the maximum number of clients supported on the port when MAC-based 802.1x authentication is enabled on the port. Use the `no` version of the command to reset the maximum number of clients supported on the port when MAC-based 802.1x authentication is enabled on the port.

Syntax

```
dot1x max-users users
no dot1x max-users
```

- `users` — The number of users the port supports for MAC-based 802.1x authentication (Range: 1–64)

Default Configuration

The default number of clients supported on a port with MAC-based 802.1x authentication is 64. The N1100-ON and N1500 Series switches, the range is 1–32.

Command Mode

Interface Configuration (Ethernet) mode
User Guidelines

The N1100-ON and N1500 Series switches support up to 32 users per interface.

Example

The following command limits the number of devices that can authenticate on port gigabitethernet 1/0/2 to 3.

```
console(config-if-Gi1/0/2)#dot1x max-users 3
```

dot1x port-control

Use the `dot1x port-control` command in Interface Configuration mode to configure the 802.1x mode of authentication on the port. Use the `no` form of the command to return the mode to the default.

Syntax

```
dot1x port-control {force-authorized | force-unauthorized | auto | mac-based}
```

```
no dot1x port-control
```

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the switch and the client. Once the first data client is authenticated, any other clients on the interface have access to the data VLAN. This is equivalent to IEEE 802.1X port-based mode. VLAN assignment is allowed on the port if it is not configured in trunk mode. This is the default port-control authentication method.

- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client. VLAN assignment is not supported in this mode.
• **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. VLAN assignment is not supported in this mode.

• **mac-based** — Enables 802.1x authentication on the interface and allows multiple hosts to individually authenticate on a single port. The hosts are distinguished by their MAC addresses and each host must authenticate independently. VLAN assignment per host is allowed on the port if it is configured in General mode.

**Default Configuration**
The default port-control mode is **auto**.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**
It is recommended that you disable spanning tree or enable spanning-tree portfast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations) in order to go immediately to the forwarding state after successful authentication.

When configuring a port to use MAC-based authentication, the port must be in switchport general mode.

**Example**
The following command enables MAC-based authentication on port 1/0/2

```
console(config)# interface gigabitethernet 1/0/2
console(config-if-Gi1/0/2)# dot1x port-control mac-based
```

**dot1x re-authenticate**
Use the **dot1x re-authenticate** command to manually initiate a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.
Syntax

dot1x re-authenticate [gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port]

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

Interfaces that are not running the 802.1x protocol (e.g. MAB configured ports) are not re-authenticated. Only ports that have an authentication dot1x port-control mode of auto are re-authenticated. This command does not cause the switch to attempt to contact RADIUS servers marked dead.

Example

The following command manually initiates a reauthentication of the 802.1x-enabled port.

console# dot1x re-authenticate gigabitethernet 1/0/16

**dot1x reauthentication**

Use the dot1x reauthentication command in Interface Configuration mode to enable periodic re-authentication of the client. To return to the default setting, use the no form of this command.

Syntax

dot1x reauthentication

no dot1x reauthentication

Default Configuration

Periodic reauthentication is disabled.
**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

It is possible to configure the periodic re-authentication timer by sending the IETF Session-Timeout attribute in the RADIUS Access-Accept. If periodic re-authentication is not enabled, the session will be terminated and the 802.1X client will need to authenticate again to access the network.

If re-authentication is enabled, the switch will initiate re-authentication and terminate the session only if the client fails re-authentication.

**Example**

The following example enables periodic reauthentication of the client.

```
console(config)# interface gigabitethernet 1/0/16
console(config-if-Gi1/0/16)# dot1x reauthentication
```

**dot1x system-auth-control**

Use the `dot1x system-auth-control` command in Global Configuration mode to enable 802.1x globally. To disable 802.1x globally, use the `no` form of this command.

**Syntax**

- `dot1x system-auth-control`
- `no dot1x system-auth-control`

**Default Configuration**

The default for this command is disabled.

**Command Mode**

Global Configuration mode
**User Guidelines**

Devices connected to interfaces on which IEEE 802.1X authentication is enabled will be required to authenticate before accessing network resources. This command enables 802.1X authentication on all interfaces, including uplinks. Use the interface mode `dot1x port-control force-authorized` command to disable 802.1X on an interface.

This command enables local processing of IEEE 802.1x frames on the switch. Dot1x eapolflood mode must be disabled for local processing to occur.

If 802.1x is used in combination with the authentication manager, be sure to enable the authentication manager with the `authentication enable` command.

**Example**

The following example enables 802.1x globally.

```
console(config)# dot1x system-auth-control
```

**dot1x system-auth-control monitor**

Use the `dot1x system-auth-control monitor` command in Global Configuration mode to enable 802.1x monitor mode globally. To disable this function, use the `no` form of this command.

**Syntax**

```
dot1x system-auth-control monitor
no dot1x system-auth-control monitor
```

**Default Configuration**

Dot1x monitor mode is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Monitor mode always allows access to network resources, even if authentication fails.
Example
The following command enables monitor mode. Clients are always authenticated in monitor mode.

    console(config)# dot1x system-auth-control monitor

dot1x timeout quiet-period

Use the dot1x timeout quiet-period command in Interface Configuration mode to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default setting, use the no form of this command.

Syntax

dot1x timeout quiet-period seconds

no dot1x timeout quiet-period

- seconds — Time in seconds that the switch remains in the quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

Default Configuration

The switch remains in the quiet state for 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the switch does not accept or initiate any authentication requests.

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, enter a smaller number than the default.
Example
The following example sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange to 3600.

```
console(config)# interface gigabitethernet 1/0/16
console(config-if-Gi1/0/16)# dot1x timeout quiet-period 3600
```

**dot1x timeout re-authperiod**

Use the `dot1x timeout re-authperiod` command in Interface Configuration mode to set the number of seconds between reauthentication attempts. To return to the default setting, use the `no` form of this command.

**Syntax**

```
dot1x timeout re-authperiod seconds
no dot1x timeout re-authperiod
```

- seconds — Number of seconds between re-authentication attempts.
  (Range: 300–4294967295)

**Default Configuration**

The default re-authentication period is 3600 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

The re-authentication process sends an authentication message (EAP-Request/Identity) to authenticated supplicants asking them to re-authenticate themselves. If a supplicant fails re-authentication, it is denied access to switch resources. Re-authentication must be enabled for this setting to have any effect.

**Example**

The following example sets the number of seconds between re-authentication attempts to 300.

```
console(config)# interface gigabitethernet 1/0/16
console(config-if-Gi1/0/16)# dot1x timeout re-authperiod 300
```
**dot1x timeout server-timeout**

Use the `dot1x timeout server-timeout` command in Interface Configuration mode to set the time that the switch waits for a response from the authentication server. To return to the default setting, use the `no` form of this command.

**Syntax**

```
dot1x timeout server-timeout seconds
```

```
no dot1x timeout server-timeout
```

- `seconds` — Time in seconds that the switch waits for a response from the authentication server. (Range: 1–65535)

**Default Configuration**

The period of time is set to 30 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

The actual timeout is this parameter or the product of the RADIUS transmission times the RADIUS timeout, whichever is smaller.

**Example**

The following example sets the time for the retransmission to the authentication server to 3600 seconds.

```
console(config-if-gi1/0/1)# dot1x timeout server-timeout 3600
```

**dot1x timeout supp-timeout**

Use the `dot1x timeout supp-timeout` command to set the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP-Request/Identity) frame to the client. To return to the default setting, use the `no` form of this command.
Syntax

dot1x timeout supp-timeout seconds

no dot1x timeout supp-timeout

- seconds—The time in seconds that the switch should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1–65535)

Default Configuration

The default supplicant timeout is 30 seconds.

Command Mode

Interface Configuration mode

User Guidelines

Change the value of the supplicant timeout only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers. The default timeout value is set per IEEE 802.1x.

This value is used in conjunction with the dot1x timeout server-timeout command to limit the amount of time a supplicant can remain in a pending authentication state.

Example

console(config-if-Gi1/0/1)#dot1x timeout supp-timeout 60

dot1x timeout tx-period

Use the dot1x timeout tx-period command in Interface Configuration mode to set the number of seconds that the switch waits for a response to an Extensible Authentication Protocol EAP-Request/Identity frame from the client before resending the request. To return to the default setting, use the no form of this command.

Syntax

dot1x timeout tx-period seconds
no dot1x timeout tx-period

- seconds — Time in seconds that the switch should wait for a response to an EAP-Request/Identity frame from the client before resending the request. (Range: 1–65535)

**Default Configuration**

The period of time is set to 30 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Example**

The following command sets the number of seconds that the switch waits for a response to an EAP-request/identity frame to 3600 seconds.

```
console(config)# interface gigabitethernet 1/0/16
console(config-if-Gi1/0/16)# dot1x timeout tx-period 3600
```

**auth-type**

Use this command to set the accepted authorization types for dynamic RADIUS clients. Use the `no` form of the command to set the authorization type to the default (all).

**Syntax**

`auth-type { all | any | session-key}`

`no auth-type`

- all—Selects all COA client authentication types. All session identification attributes must match for the authentication to succeed.
- any—Selects any COA client authentication type. Any session identification attribute may match for the authentication to succeed.
• session-key—Indicates that the session-key (Acct-Session-ID) must match for authentication to succeed.

Default Configuration
The default is to authenticate with all received session identification parameters.

Command Modes
Dynamic RADIUS Configuration

User Guidelines
This command specifies the session identification attributes to validate before acting on a CoA disconnect request. The any/all parameter only applies to the received attributes. It does not mandate which attributes must be contained in the received message. If session-key is specified and the received session ID (Acct-Session-ID) is valid, authentication succeeds even if the session-key does not match. If authentication succeeds and the session-key does not match, a response (Disconnect-NAK) will be sent. If authentication does not succeed, no response is sent.

This command works in concert with the ignore command. The ignore command refines the all parameter to limit the attribute matching.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-radius-da)# auth-type all

client
Use this command to enter the CoA client parameters.

Syntax
client {ip-address | hostname } [ server-key [0 | 7] key-string ]
no client {ip-address | hostname }
• ip-address—The IPv4 address of a CoA client. The IPv4 address is entered in dotted-quad notation.
• hostname—The fully qualified domain name (FQDN) of a CoA client. Maximum length of a host FQDN is 255 characters.
• server-key —Sets the shared secret to verify client COA requests for this server.
  • 0—An unencrypted key is to be entered.
  • 7—An encrypted key is to be entered.
• key-string—The key string in encrypted or unencrypted form. In encrypted form, it must be 256 characters in length. In unencrypted form, it may be up to 128 characters in length. Enclose in key string in quotes to use special characters or embedded blanks.

Default Configuration
By default, no dynamic CoA clients are configured.

Command Modes
Dynamic RADIUS Configuration

User Guidelines
Up to 10 dynamic CoA clients can be configured.
The server-key, if configured, overrides the global shared secret for this client only.
Messages received from a dynamic RADIUS client are validated against the configured servers. Messages received from unconfigured dynamic RADIUS clients are silently discarded.

Command History
Introduced in version 6.2.0.1 firmware.

Example
The following example configures RADIUS servers at 1.1.1.1, 2.2.2.2, and 3.3.3.3 and CoA clients at 3.3.3.3, 4.4.4.4, and 5.5.5.5. It sets the front panel ports to use 802.1x MAC-based authentication. CoA is configured for two
RADIUS servers located at 1.1.1.1 and 2.2.2.2 using a global shared secret and a third server using a server specific shared secret. CoA disconnect requests are accepted from these servers. Any session identification attribute is allowed for CoA disconnect requests.

```console
console#configure terminal
console(config)# aaa new-model
console(config)# aaa authentication dot1x default radius
console(config)# dot1x system-auth-control
console(config)# interface range gi1/0/1-24
console(config-if)# dot1x port-control mac-based
console(config-if)# exit
console(config)# radius server auth 1.1.1.1
console(config-auth-radius)#primary
console(config-auth-radius)#exit
console(config)# server auth 2.2.2.2
console(config-auth-radius)#exit
console(config)# server auth 3.3.3.3
console(config-auth-radius)#key “That’s your secret.”
console(config-auth-radius)#exit
console(config)# radius server key “Keep it. Keep it.”
console(config)# aaa server radius dynamic-author
console(config-radius-da)# client 3.3.3.3 server-key 0 “That’s your secret.”
console(config-radius-da)# client 4.4.4.4
console(config-radius-da)# client 5.5.5.5
console(config-radius-da)# server-key 0 “Keep it. Keep it.”
console(config-radius-da)# port 3799
console(config-radius-da)# auth-type any
console(config-radius-da)# exit
console(config)#dot1x system-auth-control
console(config)#dot1x initialize
```

**ignore**

Use this command to set the switch to ignore certain authentication/session identification parameters from dynamic RADIUS clients. Use the `no` form of the command to restore checking of the specific authentication parameters as configured by the `auth-type` command.

**Syntax**

```
ignore {session-key | server-key}
no ignore {session-key | server-key}
```

- Session-key—Do not attempt to authenticate with the session key.
• Server-key—Do not attempt to authenticate with the server key.

Default Configuration
The default is to authenticate using all parameters present in the received message as specified by the configured auth-type.

Command Modes
Dynamic RADIUS Configuration

User Guidelines
This command specifies the attributes to validate before acting on a CoA or disconnect request. If session-key is specified and the session ID is valid, authentication succeeds even if the session-key does not match. If the session-key (Acct-Session-ID) does not match, a Disconnect-ACK is sent. The ignore command refines the all parameter to limit the attribute matching. Setting the auth-type to session-key in conjunction with setting the ignore session-key is invalid and causes all configured servers to authenticate with no warnings.

Command History
Introduced in version 6.2.0.1 firmware.

Example
c console(config-radius-da)# ignore session-key

port
Use this command to set the port on which to listen for CoA and disconnect requests from authorized dynamic RADIUS clients.

Syntax
port port–number
no port
• port-number—An integer in the range of 1025–65535
**Default Configuration**

The default is port 3799.

**Command Modes**

Dynamic RADIUS Configuration

**User Guidelines**

Only one port may be defined and it is used to all RADIUS clients. Do not use a port number reserved for use by the switch. UDP, TCP and RAW Ports reserved by the switch and unavailable for use or configuration are:

Ports 1, 17, 58, 255, 546, 547, 2222, 4567, 6343, 49160

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-radius-da)# port 1700
```

**server-key**

Use this command to configure a global shared secret that is used for all dynamic RADIUS clients that do not have an individual shared secret configured. Use the `no` form of the command to remove the global shared secret configuration.

**Syntax**

```
server-key [0 | 7] key-string
no server-key
```

- **0**—An unencrypted key is to be entered.
- **7**—An encrypted key is to be entered.
- **key-string**—The key string in encrypted or unencrypted form. In encrypted form, it must be 256 characters in length. In unencrypted form, it may be up to 128 characters in length. Enclose the key string in quotes to use special characters or embedded blanks.
**Default Configuration**

By default, no global server key is configured.

**Command Modes**

Dynamic RADIUS Configuration

**User Guidelines**

Only one global server key may be defined. Use the server-key parameter in the `client` command to configure a unique server key for each client.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

The following example configures RADIUS servers at 1.1.1.1, 2.2.2.2, and 3.3.3.3. It sets the front panel ports to use 802.1x MAC-based authentication. CoA is configured for two RADIUS servers located at 1.1.1.1 and 2.2.2.2 using a global shared secret and a third server 3.3.3.3 using a server specific shared secret. CoA disconnect requests are accepted from these servers. Any authentication type is allowed for CoA disconnect requests.

```plaintext
console#configure terminal
console(config)# aaa new-model
console(config)# aaa authentication dot1x default radius
console(config)# dot1x system-auth-control
console(config)# interface range gi1/0/1-24
console(config-if)# dot1x port-control mac-based
console(config-if)# exit
console(config)# radius server auth 1.1.1.1
console(config-auth-radius)#primary
console(config-auth-radius)#exit
console(config)# radius server auth 2.2.2.2
console(config-auth-radius)#exit
console(config)# radius server auth 3.3.3.3
console(config-auth-radius)#key "That's your secret."
console(config-auth-radius)#exit
console(config)# radius server key "Keep it. Keep it."
console(config)# aaa server radius dynamic-author
console(config-radius-da)# client 3.3.3.3 server-key 0 "That’s your secret."
console(config-radius-da)# client 1.1.1.1
console(config-radius-da)# client 2.2.2.2
```
console(config-radius-da)# server-key 0 "Keep it. Keep it."
console(config-radius-da)# port 3799
console(config-radius-da)# auth-type any
console(config-radius-da)# exit
console(config)#dot1x system-auth-control
console(config)#dot1x initialize

**show dot1x**

Use the `show dot1x` command to display:

- A summary of the global dot1x configuration.
- Summary information of the dot1x configuration for a specified port or all ports.
- Detailed dot1x configuration for a specified port
- Dot1x statistics for a specified port, depending on the tokens used.

**Syntax**

`show dot1x [interface interface-id [statistics]]`

- `interface-id`—Any valid interface. See Interface Naming Conventions for interface representation.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

If you do not use the optional parameters, the command displays the global dot1x mode, Dynamic VLAN Creation Mode, Monitor Mode, EAPOL Flood Mode, and the VLAN Assignment mode.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>Indicates whether authentication control on the switch is enabled or disabled.</td>
</tr>
</tbody>
</table>
Example

console(config-if-Gi1/0/1)#show dot1x

Administrative Mode............. Disabled
Dynamic VLAN Creation Mode...... Disabled
VLAN Assignment Mode............ Disabled
Monitor Mode..................... Disabled
EAPOL Flood Mode................ Disabled

Port      Admin Mode         Oper Mode    Reauth   Reauth
Control   Period
--------- ------------------ ------------ -------- ----------
Gi1/0/1   auto               N/A          FALSE    3600
Gi1/0/2   auto               N/A          FALSE    3600
Gi1/0/3   auto               N/A          FALSE    3600

MAB Request Fmt Attr1 Groupsize... 2
MAB Request Fmt Attr1 Separator... legacy(:)
MAB Request Fmt Attr1 Case........ uppercase

show dot1x authentication-history

Use the show dot1x authentication-history command to display the dot1x authentication events and information during successful and unsuccessful dot1x authentication processes. The command is available to display all events, or events per interface, or only failure authentication events in summary or in detail.

Syntax

show dot1x authentication-history {interface-id | all} [failed-auth-only] [detail]
- interface-id—Any valid interface. See Interface Naming Conventions for interface representation.
- all—All interfaces.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Stamp</td>
<td>Exact time at which the event occurs.</td>
</tr>
<tr>
<td>Interface</td>
<td>Ethernet interface on which the event occurs.</td>
</tr>
<tr>
<td>MAC-Address</td>
<td>Supplicant/Client MAC Address</td>
</tr>
<tr>
<td>VLAN assigned</td>
<td>VLAN assigned to the client/port on authentication.</td>
</tr>
<tr>
<td>VLAN assigned Reason</td>
<td>Type of VLAN ID assigned i.e Guest VLAN, Unauth, Default, RADIUS Assigned or Monitor Mode VLAN ID.</td>
</tr>
<tr>
<td>Auth Status</td>
<td>Authentication Status</td>
</tr>
<tr>
<td>Reason</td>
<td>Actual reason behind the successful or failure authentication.</td>
</tr>
<tr>
<td>Result Age</td>
<td>Time since last result.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>The name of the assigned filter (policy map).</td>
</tr>
</tbody>
</table>

**Example**

```
console#show dot1x authentication-history all detail

Time Stamp......................... Mar 22 2010 01:16:31
Result Age......................... 0 days, 1 hours, 17 minutes, 38 seconds
Interface.......................... Gi1/0/2
MAC-Address......................... 00:01:02:03:04:05
VLAN Assigned....................... 111
VLAN Assigned Reason.............. Guest VLAN
```
Filter Name..........................
Auth Status.......................... Authorized
Reason.............................. Dot1x Authentication due to Guest VLAN Timer Expiry.

......
......

custom#show dot1x authentication-history all
Time Stamp            Interface MAC-Address       VLANID Auth Status
--------------------- --------- ----------------- ------ ----------
Mar 22 2010 01:16:31  Gi1/0/2   00:01:02:03:04:05 111    Authorized
Mar 22 2010 01:20:33  Gi1/0/7   00:00:0D:00:00:00 222    Authorized

custom#show dot1x authentication-history gi1/0/1
Time Stamp            Interface MAC-Address       VLANID Auth Status
--------------------- --------- ----------------- ------ ----------
Mar 22 2010 01:16:31  Gi1/0/1   00:01:02:03:04:05 111    Authorized
Mar 22 2010 01:18:22  Gi1/0/1   00:00:00:03:04:05 0      Unauthorized

custom#show dot1x authentication-history gi1/0/1 failed-auth-only
Time Stamp            Interface MAC-Address       VLANID Auth Status
--------------------- --------- ----------------- ------ ----------
Mar 22 2010 01:18:22  Gi1/0/2   00:00:00:03:04:05 0      Unauthorized

show dot1x clients

Use the show dot1x clients command to display 802.1x client information. The client information is displayed in summary or in detail. The command also displays the statistics of the number of clients that are authenticated using Monitor Mode and using 802.1x.

Syntax
show dot1x clients {interface–id | all}


Default Configuration
This command has no default configuration.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed by this command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients Authenticated using Monitor Mode</td>
<td>Indicates the number of Dot1x clients authenticated using Monitor mode.</td>
</tr>
<tr>
<td>Clients Authenticated using Dot1x</td>
<td>Indicates the number of Dot1x clients authenticated using 802.1x authentication process.</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The port number.</td>
</tr>
<tr>
<td>Username</td>
<td>The username representing the identity of the Supplicant. This field shows the username when the port control is <strong>auto</strong> or <strong>mac-based</strong>. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.</td>
</tr>
<tr>
<td>Supp MAC Address</td>
<td>The MAC-address of the supplicant</td>
</tr>
<tr>
<td>Session Time</td>
<td>The amount of time, in seconds, since the client was authenticated on the port.</td>
</tr>
<tr>
<td>Filter ID</td>
<td>The Filter ID assigned to the client by the RADIUS server. This field is not applicable when the Filter-ID feature is disabled on the RADIUS server or client. The Filter ID contains the name of a DiffServ Policy only. It does not contain the name of a DACL.</td>
</tr>
</tbody>
</table>
### Example

The following example displays information about the 802.1x clients.

```console
console#show dot1x clients all
Clients Authenticated using Monitor Mode...... 1
Clients Authenticated using Dot1x.............. 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DACL Name</td>
<td>The voice VLAN Dynamic IPv4 or IPv6 ACL or the data VLAN IPv4 or IPv6 Dynamic ACL. The Static keyword indicates that a pre-configured ACL was assigned. The downloadable keyword indicates that the ACL definition was sent in the Access-Accept.</td>
</tr>
<tr>
<td>VLAN Assigned</td>
<td>The VLAN assigned to the client by the radius server. When VLAN assignments are disabled, RADIUS server does not assign any VLAN to the port, and this field is set to 0.</td>
</tr>
<tr>
<td>RADIUS Framed IPv4 Address</td>
<td>The IPv4 address of the 802.1X client received in the Access-Accept message, if any.</td>
</tr>
<tr>
<td>RADIUS Framed IPv6 Address</td>
<td>The IPv6 address of the 802.1X client received in the Access-Accept message, if any.</td>
</tr>
</tbody>
</table>
```

```console
console#show dot1x clients all
Clients Authenticated using Monitor Mode...... 1
Clients Authenticated using Dot1x.............. 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Supp MAC Address</th>
<th>Session Time</th>
<th>Filter Id</th>
<th>DACL Name</th>
<th>RADIUS Framed IPv4/IPv6 address</th>
<th>VLAN Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/2</td>
<td>000102030405</td>
<td>518</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>00:08:A1:7E:45:1A</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```console
console#show dot1x clients all
Clients Authenticated using Monitor Mode...... 1
Clients Authenticated using Dot1x.............. 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Supp MAC Address</th>
<th>Session Time</th>
<th>Filter Id</th>
<th>DACL Name</th>
<th>RADIUS Framed IPv4/IPv6 address</th>
<th>VLAN Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/2</td>
<td>000102030405</td>
<td>518</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>00:08:A1:7E:45:1A</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
This example shows two clients with IPv4 and IPv6 dynamic ACLs authenticated on a single port. If the Dynamic ACL refers to a pre-configured ACL, the word (static) will appear after the name. If the DACL definition was received in the RADIUS Access-Accept, the word (Downloadable) appears after the name.

console#show dot1x clients all

Clients Authenticated using Monitor Mode...... 0
Clients Authenticated using Dot1x.............. 2
Interface...................................... Gi1/0/9
User Name...................................... CP-7945G-SEP0008308B02DE
Supp MAC Address............................... 0008.308B.02DE
Session Time................................... 93
Filter Id......................................
DACL Name...................................... IPV6-VDACL-IN-Gi1/0/9(Downloadable)
DACL Name...................................... IP-VDACL-IN-Gi1/0/9(Downloadable)
RADIUS Framed IPv4/IPv6 address................
VLAN Assigned.................................. 100

Interface...................................... Gi1/0/9
User Name...................................... hp
Supp MAC Address............................... ECF4.BB68.CF65
Session Time................................... 93
Filter Id......................................
DACL Name...................................... IPV6-DACL-IN-Gi1/0/9(Downloadable)
DACL Name...................................... IP-DACL-IN-Gi1/0/9(Downloadable)
RADIUS Framed IPv4/IPv6 address................
VLAN Assigned.................................. 1

show dot1x interface

This command shows the status and configuration of an IEEE 802.1x configured interface.

Syntax

show dot1x interface interface-id
Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
The command accepts Ethernet interface identifiers.

Example
console#show dot1x interface gigabitethernet 1/0/10

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
<th>Reauth Control</th>
<th>Reauth Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/10</td>
<td>auto</td>
<td>N/A</td>
<td>FALSE</td>
<td>3600</td>
</tr>
</tbody>
</table>

Quiet Period................................... 60
Transmit Period.................................. 30
Maximum Request-Identities...................... 2
Maximum Requests.................................. 2
Max Users....................................... 64
VLAN Assigned....................................
Supplicant Timeout............................... 30
Guest-vlan Timeout............................... 90
Server Timeout (secs)............................ 30
MAB mode (configured)............................ Disabled
MAB mode (operational)........................... Disabled
MAB Protocol.................................... EAP
Authentication Server Dead action for Voice.... None
Authentication Server Alive action............. None
Authenticator PAE State.......................... Initialize
Backend Authentication State................... Idle
show dot1x interface statistics

Use the `show dot1x interface statistics` command to display 802.1x statistics for the specified interface.

**Syntax**

```
show dot1x interface {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port} statistics
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface for which counters are displayed.</td>
</tr>
<tr>
<td>EAPOL Frames Received</td>
<td>The number of valid EAPOL frames of any type that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EAPOL Frames Transmitted</td>
<td>The number of EAPOL frames of any type that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EAPOL Start Frames Received</td>
<td>The number of EAPOL Start frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EAPOL Logoff Frames Received</td>
<td>The number of EAPOL Logoff frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EAP Response/ID Frames Received</td>
<td>The number of EAP Resp/Id frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EAP Response Frames Received</td>
<td>The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.</td>
</tr>
</tbody>
</table>
The following example displays 802.1x statistics for the specified interface.

```
console#show dot1x interface gigabitethernet 1/0/2 statistics
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP Request/ID Frames Transmitted</td>
<td>The number of EAP Req/Id frames that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EAP Request Frames Transmitted</td>
<td>The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>Invalid EAPOL Frames Received</td>
<td>The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAPOL Length Error Frames Received</td>
<td>The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.</td>
</tr>
<tr>
<td>Last EAPOL Frame Version</td>
<td>The protocol version number carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>Last EAPOL Frame Source</td>
<td>The source MAC address carried in the most recently received EAPOL frame.</td>
</tr>
</tbody>
</table>

**Example**

The following example displays 802.1x statistics for the specified interface.

```
console#show dot1x interface gigabitethernet 1/0/2 statistics
```

<table>
<thead>
<tr>
<th>Port.........................................</th>
<th>Gi1/0/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPOL Frames Received........................</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Frames Transmitted....................</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Start Frames Received.................</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Logoff Frames Received................</td>
<td>0</td>
</tr>
<tr>
<td>Last EAPOL Frame Version...................</td>
<td>0</td>
</tr>
<tr>
<td>Last EAPOL Frame Source....................</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>EAP Response/Id Frames Received............</td>
<td>0</td>
</tr>
<tr>
<td>EAP Response Frames Received..............</td>
<td>0</td>
</tr>
<tr>
<td>EAP Request/Id Frames Transmitted.........</td>
<td>0</td>
</tr>
<tr>
<td>EAP Request Frames Transmitted............</td>
<td>0</td>
</tr>
<tr>
<td>Invalid EAPOL Frames Received.............</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Length Error Frames Received........</td>
<td>0</td>
</tr>
</tbody>
</table>

**show dot1x users**

Use the `show dot1x users` command to display 802.1x authenticated users for the switch.
Syntax

show dot1x users [username username]

- username — Supplicant username (Range: 1–64 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x users.

```
console#show dot1x users
Port     Username
--------  --------
Gi1/0/1   Bob
Gi1/0/2   John
Switch# show dot1x users username Bob
Port     Username
--------  --------
Gi1/0/1   Bob
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username representing the identity of the Supplicant.</td>
</tr>
<tr>
<td>Port</td>
<td>The port over which the user authenticated.</td>
</tr>
</tbody>
</table>

**clear dot1x authentication-history**

Use the `clear dot1x authentication-history` command to clear the authentication history table captured during successful and unsuccessful authentication.
Syntax

clear dot1x authentication-history [interface-id]

- interface-id—Any valid interface. See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

This command has no user guidelines.

Example

This examples clears all entries from the authentication log.

```
console#clear dot1x authentication-history
```

This example purges all entries for the specified interface from the authentication log.

```
console#clear dot1x authentication-history gi1/0/1
```

802.1x Advanced Features

dot1x guest-vlan

Use the dot1x guest-vlan command in Interface Configuration mode to set the guest VLAN on a port. The VLAN must be defined prior to use. The no form of this command sets the guest VLAN id to zero, which disables the guest VLAN on a port.

Syntax

dot1x guest-vlan vlan-id

no dot1x guest-vlan
• **vlan-id** — The ID of a valid VLAN to use as the guest VLAN (Range: 1-4093).

**Default Configuration**

The guest VLAN is disabled on the interface by default.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

If configured, the guest VLAN is the VLAN to which 802.1X unaware clients are assigned. Configure the guest VLAN before using this command.

By default, the switch retries authentication one time before assigning a supplicant to the guest VLAN.

**Example**

The following example sets the guest VLAN on port 1/0/2 to VLAN 10.

```
console(config-if-Gi1/0/2)#dot1x guest-vlan 10
```

**dot1x timeout guest-vlan-period**

Use the `dot1x timeout guest-vlan-period` command in Interface Configuration mode to set the number of seconds that the switch waits before authorizing the client if the client is a 802.1X unaware client. Use the `no` form of the command to return the timeout to the default value.

**Syntax**

```
dot1x timeout guest-vlan-period seconds
no dot1x timeout guest-vlan-period
```

- **seconds** — Time in seconds that the switch waits before authorizing the client if the client is a 802.1X unaware client. Range 1-300.

**Default Configuration**

The switch remains in the quiet state for 90 seconds.
**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

It is recommended that the user set the dot1x timeout guest-vlan-period to at least three times the dot1x timeout tx-period timer so that at least three EAP Requests are sent, before assuming that the client is an 802.1X unaware client. An 802.1X unaware client is one that does not respond to EAP-Request/Identity frames and does not send EAPOL-Start or EAP-Response/Identity frames.

**Example**

The following example sets the 802.1X timeout guest vlan period to 100 seconds.

```
console(config)# dot1x timeout guest-vlan-period 100
```

**dot1x unauth-vlan**

Use the dot1x unauth-vlan command in Interface Configuration mode to specify the unauthenticated VLAN on a port. The unauthenticated VLAN is the VLAN to which supplicants that fail 802.1x authentication are assigned.

**Syntax**

```
dot1x unauth-vlan vlan-id
no dot1x unauth-vlan
```

- **vlan-id** — The ID of a valid VLAN to use for unauthenticated clients (Range: 1-4093).

**Default Configuration**

The unauthenticated VLAN is disabled on the interface by default.

**Command Mode**

Interface Configuration (Ethernet) mode
**User Guidelines**

By default, the switch will retry authentication one time before assigning a user to the unauthenticated VLAN. Configure the unauthenticated VLAN before using this command.

**Example**

The following example set the unauthenticated VLAN on port 1/0/2 to VLAN 20.

```
console(config-if-Gi1/0/2)#dot1x unauth-vlan 20
```

**show dot1x advanced**

Use the `show dot1x advanced` command to display 802.1x advanced features for the switch or for the specified interface. The output of this command has been updated in release 2.1 to remove the Multiple Hosts column and add an Unauthenticated VLAN column, which indicates whether an unauthenticated VLAN is configured on a port. The command has also been updated to show the Guest VLAN ID (instead of the status) since it is now configurable per port.

**Syntax**

```
show dot1x advanced [{gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays 802.1x advanced features for the switch.
```
console#show dot1x advanced
Port        Guest       Unauthenticated
            VLAN             Vlan
---------   ---------   ---------------
Gi1/0/1     Disabled    Disabled
Gi1/0/2     10          20
Gi1/0/3     Disabled    Disabled
Gi1/0/4     Disabled    Disabled
Gi1/0/5     Disabled    Disabled
Gi1/0/6     Disabled    Disabled

console#show dot1x advanced gigabitethernet 1/0/2
Port        Guest       Unauthenticated
            VLAN             Vlan
---------   ---------   ---------------
Gi1/0/2     10          20
```
Captive Portal Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Captive Portal feature is a software implementation that blocks both wired and wireless clients from accessing the network until user verification has been established. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

The Authentication server supports both HTTP and HTTPS web connections. In addition, Captive Portal can be configured to use an optional HTTP port (in support of HTTP Proxy networks) or an optional HTTPS port. If configured, this additional port or ports are then used exclusively by Captive Portal.

NOTE: This optional HTTP port is in addition to the standard HTTP port 80 which is currently being used for all other web traffic, and the optional HTTPS port is in addition to the standard HTTPS port 443 used for secure web traffic.

Commands in this Section

This section explains the following commands:

**Administrative Profiles Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication timeout</td>
<td>https port</td>
</tr>
<tr>
<td>captive-portal</td>
<td>show captive-portal</td>
</tr>
<tr>
<td>enable</td>
<td>show captive-portal status</td>
</tr>
<tr>
<td>http port</td>
<td></td>
</tr>
</tbody>
</table>

**Captive Portal Configuration Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>name (Captive Portal)</td>
</tr>
<tr>
<td>configuration</td>
<td>protocol</td>
</tr>
<tr>
<td>enable</td>
<td>redirect</td>
</tr>
<tr>
<td>group</td>
<td>redirect-url</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>interface</td>
<td>session-timeout</td>
</tr>
<tr>
<td>locale</td>
<td>verification</td>
</tr>
</tbody>
</table>

### Captive Portal Client Connection Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal client deauthenticate</td>
<td>show captive-portal interface client status</td>
</tr>
<tr>
<td>show captive-portal client status</td>
<td>show captive-portal interface configuration status</td>
</tr>
<tr>
<td>show captive-portal configuration client status</td>
<td>–</td>
</tr>
</tbody>
</table>

### Captive Portal Local User Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear captive-portal users</td>
<td>user-logout</td>
</tr>
<tr>
<td>no user</td>
<td>user name</td>
</tr>
<tr>
<td>show captive-portal user</td>
<td>user password</td>
</tr>
<tr>
<td>user group</td>
<td>user session-timeout</td>
</tr>
</tbody>
</table>

### Captive Portal Status Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show captive-portal configuration</td>
<td>show captive-portal configuration locales</td>
</tr>
<tr>
<td>show captive-portal configuration interface</td>
<td>show captive-portal configuration status</td>
</tr>
</tbody>
</table>

### Captive Portal User Group Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user group</td>
<td>user group name</td>
</tr>
<tr>
<td>user group moveusers</td>
<td>–</td>
</tr>
</tbody>
</table>
Captive Portal Global Commands

authentication timeout

Use the authentication timeout command to configure the authentication timeout. If the user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network. Use the “no” form of this command to reset the authentication timeout to the default.

Syntax

authentication timeout timeout
no authentication timeout
  • timeout—The authentication timeout (Range: 60–600 seconds).

Default Configuration

The default authentication timeout is 300 seconds.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

captive-portal

Use the captive-portal command to enter the captive portal configuration mode.

Syntax

capture-portal
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Global Configuration mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
console(config)#captive-portal
console(config-cp)#

**enable**
Use the `enable` command to globally enable captive portal. Use the “no” form of this command to globally disable captive portal.

**Syntax**
`enable`
`no enable`

**Default Configuration**
Captive Portal is disabled by default.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
console(config-cp)#enable
http port

Use the `http port` command to configure an additional HTTP port for captive portal to listen for connections. Use the “no” form of this command to remove the additional HTTP port from monitoring.

Syntax

```
http port port-num
no http port
```

- `port-num`—The port number on which the HTTP server listens for connections (Range: 1025–65535).

Default Configuration

Captive portal only monitors port 80 by default.

Command Mode

Captive Portal Configuration mode

User Guidelines

The port number should not be set to a value that might conflict with other well-known protocol port numbers used on this switch.

Example

```
console(config-cp)#http port 32768
console(config-cp)#no http port
```

https port

Use the `https port` command to configure an additional HTTPS port for captive portal to monitor. Use the “no” form of this command to remove the additional HTTPS port.

Syntax

```
https port port-num
no https port
```

• port-num—The port number on which the HTTPS server listens for connections (Range: 1025–65535).

**Default Configuration**
Captive portal listens on port 443 by default.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
The port number should not be set to a value that might conflict with other well-known protocol port numbers used on this switch.

**Example**

```
console(config-cp)#https port 1443
console(config-cp)#no https port
```

**show captive-portal**
Use the `show captive-portal` command to display the status of the captive portal feature.

**Syntax**

```
show captive-portal
```

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes.

**User Guidelines**
There are no user guidelines for this command.
**Example**

console#show captive-portal
Administrative Mode....................... Disabled
Operational Status......................... Disabled
Disable Reason............................ Administrator Disabled
CP IP Address............................. 1.2.3.4

**show captive-portal status**

Use the `show captive-portal status` command to report the status of all captive portal instances in the system.

**Syntax**

`show captive-portal status`

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

console#show captive-portal status

Additional HTTP Port....................... 81
Additional HTTP Secure Port................. 1443
Authentication Timeout..................... 300
Supported Captive Portals.................. 10
Configured Captive Portals............... 1
Active Captive Portals.................... 0
Local Supported Users...................... 128
Configured Local Users.................... 3
System Supported Users.................... 1024
Authenticatet Users....................... 0
Captive Portal Configuration Commands
The commands in this section are related to captive portal configurations.

block
Use the block command to block all traffic for a captive portal configuration. Use the “no” form of this command to unblock traffic.

Syntax
block
to block
no block

Default Configuration
Traffic is not blocked by default.

Command Mode
Captive Portal Instance mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-cp 2)#block

configuration
Use the configuration command to enter the captive portal instance mode. The captive portal configuration identified by CP ID 1 is the default CP configuration. The system supports a total of ten CP configurations. Use the “no” form of this command to delete a configuration. The default configuration (1) cannot be deleted.

Syntax
configuration cp-id	no configuration cp-id
- cp-id—Captive Portal ID (Range: 1–10).

**Default Configuration**
Configuration 1 is enabled by default.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```console
console(config-cp)#configuration 2
console(config-cp 2)#
```

**enable**
Use the `enable` command to enable a captive portal configuration. Use the `no` form of this command to disable a configuration.

**Syntax**
```plaintext
enable
no enable
```

**Default Configuration**
Configurations are enabled by default

**Command Mode**
Captive Portal Instance mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```console
console(config-cp 2)#no enable
```
**group**

Use the **group** command to configure the group number for a captive portal configuration. If a group number is configured, the user entry (Local or RADIUS) must be configured with the same name and the group to authenticate to this captive portal instance. Use the **no** form of this command to reset the group number to the default.

**Syntax**

group group-number
no group

- group-number—The number of the group to associate with this configuration (Range: 1–10).

**Default Configuration**

The default group number is 1.

**Command Mode**

Captive Portal Instance mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

custom(config-cp 2)#group 2

**interface**

Use the **interface** command to associate an interface with a captive portal configuration. Use the **no** form of this command to remove an association.

**Syntax**

interface interface
no interface interface

- interface—An interface or range of interfaces.
**Default Configuration**
No interfaces are associated with a configuration by default.

**Command Mode**
Captive Portal Instance Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-cp 2)#interface gi1/0/2
```

**locale**
The `locale` command is not intended to be a user command. The administrator must use the Web UI to create and customize captive portal web content. This command is primarily used by the `show running-config` command and process as it provides the ability to save and restore configurations using a text based format.

**Syntax**
```
locale web-id
```
- `web-id`—The locale number (Range: 1–3)

**Default Configuration**
Locale 1 is configured by default.

**Command Mode**
Captive Portal Instance mode.

**User Guidelines**
Captive Portal supports 3 locales per configuration.
name (Captive Portal)

Use the `name` command to configure the name for a captive portal configuration. Use the `no` form of this command to remove a configuration name.

**Syntax**

```
name cp-name
no name
```

- `cp-name`—CP configuration name (Range: 1–32 characters).

**Default Configuration**

Configuration 1 has the name “Default” by default. All other configurations have no name by default.

**Command Mode**

Captive Portal Instance mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config-cp 2)#name cp2
```

**protocol**

Use the `protocol` command to configure the protocol mode for a captive portal configuration.

**Syntax**

```
protocol {http | https}
```

**Default Configuration**

The default protocol mode is http.
**Command Mode**
Captive Portal Instance mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-cp 2)#protocol http
```

**redirect**
Use the `redirect` command to enable the redirect mode for a captive portal configuration. Use the “no” form of this command to disable redirect mode.

**Syntax**
```
redirect
no redirect
```

**Default Configuration**
Redirect mode is disabled by default.

**Command Mode**
Captive Portal Instance mode.

**User Guidelines**
Enabling redirect mode will configure the `redirect-url` with an empty URL.

**Example**
```
console(config-cp 2)#redirect
```

**redirect-url**
Use the `redirect-url` command to configure the redirect URL for a captive portal configuration.
Syntax
redirect-url url
  • url—The URL for redirection (Range: 1–512 characters).

Default Configuration
There is no redirect URL configured by default.

Command Mode
Captive Portal Instance mode.

User Guidelines
The administrator must enable redirect mode before executing this command.

Example
console(config-cp 2)#redirect-url www.dell.com

session-timeout
Use the session-timeout command to configure the session timeout for a captive portal configuration. Use the no form of this command to reset the session timeout to the default.

Syntax
session-timeout timeout
no session-timeout
  • timeout—Session timeout. 0 indicates timeout not enforced (Range: 0–86400 seconds).

Default Configuration
There is no session timeout by default.

Command Mode
Captive Portal Instance mode.
User Guidelines
There are no user guidelines for this command.

Example
```
console(config-cp 2)#session-timeout 86400
console(config-cp 2)#no session-timeout
```

verification
Use the verification command to configure the verification mode for a captive portal configuration.

Syntax
```
verification { guest | local | radius }
```
- **guest**—Allows access for unauthenticated users (users that do not have assigned user names and passwords).
- **local**—Authenticates users against a local user database.
- **radius**—Authenticates users against a remote RADIUS database.

Default Configuration
The default verification mode is guest.

Command Mode
Captive Portal Instance mode.

User Guidelines
There are no user guidelines for this command.

Example
```
console(config-cp 2)#verification local
```
Captive Portal Client Connection Commands

captive-portal client deauthenticate

Use the `captive-portal client deauthenticate` command to deauthenticate a specific captive portal client.

**Syntax**

captive-portal client deauthenticate macaddr

- macaddr—Client MAC address.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console#captive-portal client deauthenticate 0002.BC00.1290
```

show captive-portal client status

Use the `show captive-portal client status` command to display client connection details or a connection summary for connected captive portal users.

**Syntax**

show captive-portal client [macaddr] status

- macaddr—Client MAC address.

**Default Configuration**

There is no default configuration for this command.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show captive-portal client status
Client MAC Address     Client IP Address     Protocol     Verification     Session Time
----------------------------  -----------------     --------     ------------     ------------
0002.BC00.1290         10.254.96.47      https        Local          0d:00:01:20
0002.BC00.1291         10.254.96.48      https        Local          0d:00:05:20
0002.BC00.1292         10.254.96.49      https        Radius         0d:00:00:20
```
```
console#show captive-portal client 0002.BC00.1290 status
Client MAC Address........................ 0002.BC00.1290
Client IP Address......................... 10.254.96.47
Protocol Mode................................ https
Verification Mode............................ Local
CP ID....................................... 1
CP Name..................................... cp1
Interface.................................... Gi1/0/1
Interface Description...................... Unit: 1 Slot: 0 Port: 1 Gigabit - Level
User Name................................... user123
Session Time............................... 0d:00:00:13
```

**show captive-portal configuration client status**
Use the `show captive-portal configuration client status` command to display the clients authenticated to all captive portal configurations or a to specific configuration.

**Syntax**
```
show captive-portal configuration [ cp-id ] client status
```

- cp-id—Captive Portal ID.

**Default Configuration**
There is no default configuration for this command.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show captive-portal configuration client status
CP ID     CP Name     Client MAC Address Client IP Address Interface
----- --------------- ------------------ ----------------- ---------
   1     cp1             0002.BC00.1290     10.254.96.47      Gi1/0/1
         0002.BC00.1291     10.254.96.48      Gi1/0/2
         0002.BC00.1292     10.254.96.49      Gi1/0/3
         0002.BC00.1293     10.254.96.50      Gi1/0/4

console#show captive-portal configuration 1 client status
CP ID..................................... 1
CP Name................................... cp1
       Client           Client
       MAC Address      IP Address   Interface       Interface Description
-------------- --------------- --------- --------------------------------
0002.BC00.1290 10.254.96.47    Gi1/0/1      Unit: 1 Slot: 0 Port: 1 Gigabit
0002.BC00.1291 10.254.96.48    Gi1/0/2      Unit: 1 Slot: 0 Port: 2 Gigabit
```

**show captive-portal interface client status**
Use the `show captive-portal interface client status` command to display information about clients authenticated on all interfaces or a specific interface.

**Syntax**
```
show captive-portal interface {gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port} client status
```

**Default Configuration**
There is no default configuration for this command.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```bash
console#show captive-portal interface client status

Client                  Client
Intf                    Intf Description            MAC Address       IP Address
------ ----------------------------------- ----------------- ---------------
Gi1/0/1     Unit: 1 Slot: 0 Port: 1 Gigabit     0002.BC00.1290    10.254.96.47
Gi1/0/2     Unit: 1 Slot: 0 Port: 2 Gigabit     0002.BC00.1291    10.254.96.48
Gi1/0/3     Unit: 1 Slot: 0 Port: 3 Gigabit     0002.BC00.1292    10.254.96.49
Gi1/0/4     Unit: 1 Slot: 0 Port: 4 Gigabit     0002.BC00.1293    10.254.96.50

console#show captive-portal interface gi1/0/1 client status

Interface................................. Gi1/0/1
Interface Description..................... Unit: 1 Slot: 0 Port: 1 Gigabit

Client                        Client
MAC Address       IP Address   CP ID       CP Name     Protocol Verification
----------------- --------------- ----- ----------------- -------- ---------
0002.BC00.1290     10.254.96.47   1     cp1               http     local
0002.BC00.1291     10.254.96.48   2     cp2               http     local
```

**Captive Portal Interface Commands**

**show captive-portal interface configuration status**

Use the `show captive-portal interface configuration status` command to display the interface to configuration assignments for all captive portal configurations or for a specific configuration.

**Syntax**

`show captive-portal interface configuration [cp-id] status`

  - `cp-id`—Captive Portal ID.
Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show captive-portal interface configuration status
CP ID CP Name Interface Interface Description Type
----- -------- --------- ------------------------------------ --------
1 Default Gi1/0/1 Unit:1 Slot: 0 Port: 1 Gigabit . Physical

console#show captive-portal interface configuration 1 status
CP ID..................................... 1
CP Name................................... cp1

Interface Interface Description Type
--------- ----------------------------------- --------
Gi1/0/1 Unit: 1 Slot: 0 Port: 1 Gigabit ... Physical

Captive Portal Local User Commands

clear captive-portal users
Use the clear captive-portal users command to delete all captive portal user entries.

Syntax
clear captive-portal users

Default Configuration
There is no default configuration for this command.
**Command Mode**
Privileged Exec mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
console#clear captive-portal users

**no user**
Use the no user command to delete a user from the local user database. If the user has an existing session, it is disconnected.

**Syntax**
no user user-id
  - user-id—User ID (Range: 1–128).

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
console(config-cp)#no user 1

**show captive-portal user**
Use the show captive-portal user command to display all configured users or a specific user in the captive portal local user database.
Syntax
show captive-portal user [user-id]
  •  user-id—User ID (Range: 1–128).

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show captive-portal user

<table>
<thead>
<tr>
<th>User ID</th>
<th>User Name</th>
<th>Session Timeout</th>
<th>Group ID</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>user123</td>
<td>14400</td>
<td>1</td>
<td>Default</td>
</tr>
<tr>
<td>2</td>
<td>user234</td>
<td>0</td>
<td>1</td>
<td>Default</td>
</tr>
</tbody>
</table>

console#show captive-portal user 1
User ID........................................ 1
User Name...................................... user123
Password Configured............................ Yes
Session Timeout................................ 0

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default</td>
</tr>
<tr>
<td>2</td>
<td>group2</td>
</tr>
</tbody>
</table>

user group
Use the user group command to associate a group with a captive portal user.
Use the “no” form of this command to disassociate a group and user. A user must be associated with at least one group so the last group cannot be disassociated.
Syntax
user user-id group group-id
  • user-id—User ID (Range: 1–128).
  • group-id—Group ID (Range: 1–10).

Default Configuration
A user is associated with group 1 by default.

Command Mode
Captive Portal Configuration mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-cp)#user 1 group 3

user-logout

Use the user-logout command in Captive Portal Instance mode to enable captive portal users to log out of the portal (versus having the session time out). Use the no form of the command to return the user logout configuration to the default.

Syntax
user-logout
no user-logout

Default Configuration
User-logout is disabled by default.

Command Mode
Captive-portal Instance mode
**User Guidelines**

There are no user guidelines for this command.

**Example**

In this example, all classes of entries in the mac address-table are displayed.

```console
console(config)#captive-portal
console(config-cp)#user 1 name asd
console(config-cp)#configuration 1
console(config-cp 1)#user-logout
console(config-cp 1)#no user-logout
```

**user name**

Use the `user name` command to modify the user name for a local captive portal user.

**Syntax**

```
user user-id name name
```

- `user-id`—User ID (Range: 1–128).
- `name`—user name (Range: 1–32 characters).

**Default Configuration**

There is no name for a user by default.

**Command Mode**

Captive Portal Configuration mode.

**User Guidelines**

There are no user guidelines.

**Example**

```console
console(config-cp)#user 1 name johnsmith
```
**user password**

Use the `user password` command to create a local user or change the password for an existing user.

**Syntax**

```
user user-id password {password | encrypted enc-password}
```

- `user-id` — User ID (Range: 1–128).
- `password` — User password (Range: 8–64 characters).
- `enc-password` — User password in encrypted form.

**Default Configuration**

There are no users configured by default.

**Command Mode**

Captive Portal Configuration mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config-cp)#user 1 password
Enter password (8 to 64 characters): ********
Re-enter password: ********
```

**user session-timeout**

Use the `user session-timeout` command to set the session timeout value for a captive portal user. Use the `no` form of this command to reset the session timeout to the default.

**Syntax**

```
user user-id session-timeout timeout
no user user-id session-timeout
```

- `user-id` — User ID (Range: 1–128).
• timeout—Session timeout. 0 indicates use global configuration (Range: 0–86400 seconds).

**Default Configuration**
The global session timeout is used by default.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-cp)#user 1 session-timeout 86400
console(config-cp)#no user 1 session-timeout
```

**Captive Portal Status Commands**

**show captive-portal configuration**
Use the `show captive-portal configuration` command to display the operational status of each captive portal configuration.

**Syntax**
```
show captive-portal configuration cp-id
```
- **cp-id**—Captive Portal ID.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
There are no user guidelines for this command.

Example
console#show captive-portal configuration 1
CP ID..................................... 1
CP Name................................... cp1
Operational Status...................... Disabled
Disable Reason.......................... Administrator Disabled
Blocked Status........................... Not Blocked
Configured Locales........................ 1
Authenticated Users........................ 0

show captive-portal configuration interface
Use the show captive-portal configuration interface command to display information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration.

Syntax
show captive-portal configuration cp-id interface [{gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]
- cp-id—Captive Portal ID.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
console#show captive-portal configuration 1 interface
CP ID..................................... 1
show captive-portal configuration locales

Use the `show captive-portal configuration locales` command to display locales associated with a specific captive portal configuration.

**Syntax**

```
show captive-portal configuration cp-id locales
```

- `cp-id`—Captive Portal Configuration ID.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console#show captive-portal configuration 1 locales
Locale Code
---------------
```
show captive-portal configuration status

Use the `show captive-portal configuration status` command to display information about all configured captive portal configurations or about a specific captive portal configuration.

**Syntax**

```
show captive-portal configuration [ cp-id ] status
```

- `cp-id`—Captive Portal ID.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console#show captive-portal configuration status
<table>
<thead>
<tr>
<th>CP ID</th>
<th>CP Name</th>
<th>Mode</th>
<th>Protocol</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cp1</td>
<td>Enable</td>
<td>https</td>
<td>Guest</td>
</tr>
<tr>
<td>2</td>
<td>cp2</td>
<td>Enable</td>
<td>http</td>
<td>Local</td>
</tr>
<tr>
<td>3</td>
<td>cp3</td>
<td>Disable</td>
<td>https</td>
<td>Guest</td>
</tr>
</tbody>
</table>

console#show captive-portal configuration 1 status
<table>
<thead>
<tr>
<th>CP ID</th>
<th>CP Name</th>
<th>Mode</th>
<th>Protocol</th>
<th>Verification</th>
<th>Group Name</th>
<th>Redirect URL Mode</th>
<th>Redirect URL</th>
<th>Session Timeout (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cp1</td>
<td>Enabled</td>
<td>https</td>
<td>Guest</td>
<td>group123</td>
<td>Enabled</td>
<td><a href="http://www.cnn.com">www.cnn.com</a></td>
<td>86400</td>
</tr>
</tbody>
</table>
```
Captive Portal User Group Commands

**user group**

Use the `user group` command to create a user group. Use the `no` form of this command to delete a user group. The default user group (1) cannot be deleted.

**Syntax**

```plaintext
user group group-id
no user group group-id

group-id — Group ID (Range: 1–10).
```

**Default Configuration**

User group 1 is created by default and cannot be deleted.

**Command Mode**

Captive Portal Configuration mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```plaintext
console(config-cp)#user group 2
console(config-cp)#no user group 2
```

**user group moveusers**

Use the `user group moveusers` command to move a group’s users to a different group.

**Syntax**

```plaintext
user group group-id moveusers new-group-id

• group-id — Group ID (Range: 1–10).
• new-group-id — Group ID (Range: 1–10).
```
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Captive Portal Configuration mode

**User Guidelines**
The new group-id must already exist.

**Example**
```
console(config-cp)#user group 2
console(config-cp)#user 1 group 2
console(config-cp)#user group 2 moveusers 3
```

**user group name**
Use the `user group name` command to configure a group name.

**Syntax**
```
user group group-id name name
```
- group-id—Group ID (Range: 1–10).
- name—Group name (Range: 1–32 alphanumeric characters).

**Default Configuration**
User groups have no names by default.

**Command Mode**
Captive Portal Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-cp)#user group 2 name group2
```
Denial of Service Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Dell EMC Networking DoS capability supports a package of filters intended to provide network administrators the ability to reduce network exposure to common attack vectors. The following list shows the DoS attack detection Dell EMC Networking supports.

- **SIP=DIP:**
  - Source IP address = Destination IP address.
- **First Fragment:**
  - TCP Header size smaller then configured value.
- **TCP Fragment:**
  - IP Fragment Offset = 1.
- **TCP Flag:**
  - TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and
  - TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and
  - TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:**
  - Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:**
  - Limiting the size of ICMP Ping packets.
- **SMAC=DMAC:**
  - Source MAC address = Destination MAC address.
- **TCP Port:**
  - Source TCP Port = Destination TCP Port.
- **UDP Port:**
  - Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:**
– TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and
– TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and
– TCP Sequence Number = 0 or TCP Flags SYN and FIN set.

• TCP Offset:
  – Checks for TCP header offset = 1.

• TCP SYN:
  – TCP Flag SYN set.

• TCP SYN & FIN:
  – TCP Flags SYN and FIN set.

• TCP FIN & URG & PSH:
  – TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.

• ICMP V6:
  – Limiting the size of ICMPv6 Ping packets.

• ICMP Fragment:
  – Checks for fragmented ICMP packets.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos-control firstfrag</td>
<td>rate-limit cpu</td>
</tr>
<tr>
<td>dos-control icmp</td>
<td>show dos-control</td>
</tr>
<tr>
<td>dos-control l4port</td>
<td>show system internal pktngr</td>
</tr>
<tr>
<td>dos-control sipdip</td>
<td>storm-control broadcast</td>
</tr>
<tr>
<td>dos-control tcpflag</td>
<td>storm-control multicast</td>
</tr>
<tr>
<td>dos-control tcpfrag</td>
<td>storm-control unicast</td>
</tr>
</tbody>
</table>
**dos-control firstfrag**

Use the `dos-control firstfrag` command in Global Configuration mode to enable Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets are dropped.

**Syntax**

dos-control firstfrag [size]

no dos-control firstfrag

- size —TCP header size. (Range: 0-255). The default TCP header size is 20. ICMP packet size is 512.

**Default Configuration**

Denial of Service is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example defines a minimum TCP header size of 20. Packets entering with a smaller header size are dropped.

```
console(config)#dos-control firstfrag 20
```

**dos-control icmp**

Use the `dos-control icmp` command in Global Configuration mode to enable Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets are dropped.
Syntax

dos-control icmp [size ]
no dos-control icmp

- size — Maximum ICMP packet size. (Range: 0-16376). If size is unspecified, the value is 512.

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates the Maximum ICMP Packet Denial of Service protection with a maximum packet size of 1023.

```console
console(config)#dos-control icmp 1023
```

**dos-control l4port**

Use the **dos-control l4port** command in Global Configuration mode to enable L4 Port Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets are dropped.

Syntax

dos-control l4port
no dos-control l4port

Default Configuration

Denial of Service is disabled.
**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example activates L4 Port Denial of Service protection.

```
console(config)#dos-control l4port
```

**dos-control sipdip**
Use the `dos-control sipdip` command in Global Configuration mode to enable Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets is dropped if the mode is enabled.

**Syntax**

dos-control sipdip
dos-control sipdip

**Default Configuration**
Denial of Service is disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example activates SIP=DIP Denial of Service protection.

```
console(config)#dos-control sipdip
```
**dos-control tcpflag**

Use the `dos-control tcpflag` command in Global Configuration mode to enable TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024, having TCP Control Flags set to 0 and TCP Sequence Number set to 0, having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0, or having TCP Flags SYN and FIN both set, the packets are dropped.

**Syntax**

dos-control tcpflag

no dos-control tcpflag

**Default Configuration**

Denial of Service is disabled.

**Command Mode**

Global Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example activates TCP Flag Denial of Service protections.

```
console(config)#dos-control tcpflag
```

**dos-control tcpfrag**

Use the `dos-control tcpfrag` command in Global Configuration mode to enable TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets are dropped.

**Syntax**

dos-control tcpfrag
no dos-control tcpfrag

**Default Configuration**
Denial of Service is disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example activates TCP Fragment Denial of Service protection.
```
console(config)#dos-control tcpfrag
```

**rate-limit cpu**
Use the `rate-limit cpu` command to reduce the amount of unknown unicast/multicast packets forwarded to the CPU on CoS queues 0 and 1.
This command also configures the rate in packets-per-second for the number of IPv4 and IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved MAC address of the destination IPv6 node. Packets exceeding the rate limit are silently discarded.

Use the `no` form of the command to return the rate limit to the default value.

**Syntax**
```
rate-limit cpu direction input pps pps-value
no rate-limit cpu direction input pps
```

- pps-value—Range of 100-1024 packets per second (100-3000 for N4000 switches)

**Default Configuration**
The default is 1024 packets per second (3000 for N4000 switches)
**Command Modes**

Global Configuration mode

**User Guidelines**

Unknown multicast and IPv4/IPv6 data packets destined to hosts in the connected networks on the router for which the MAC address is not resolved are trapped to CPU to trigger the ARP/neighbor discovery resolution of those hosts.

When the ARP or neighbor table is filled, the switch cannot accommodate new entries. In this case, there is no value in receiving the unresolved IPv4/IPv6 packets. Likewise, in cases of a L2 network re-convergence, a large number of neighbors may not be discovered but may be transmitting traffic. In the case of multicast data, certain multicast topologies using multi-access VLANs may result in packets being forwarded to the CPU with no associated PIM or MFDB state.

Receiving large numbers unresolved packets spikes the CPU usage to high levels at no benefit. For IPv6, it also results in delayed processing of the NUD packets (NS/NA) for the existing neighbor entries leading to NUD anomalies and deletions of existing neighbor entries.

To avoid such an unnecessary CPU load leading to NUD anomalies when the ARP or IPV6 neighbor table is close to full (crossing 95% of table size) or other failures, the switch automatically reduces the rate limit to an empirical value of 50 pps irrespective of the configured rate limit. When the table size falls below 95% of the table size, it is restored to the configured rate limit value.

Use this command to limit the CPU load in situations where large numbers of unknown multicast or IPv4/IPv6 packets with an unknown multicast or unicast IPv4/IPv6 destination are being handled in software. The symptom can be diagnosed by high CPU usage of the ipMapForwardingTask.

**Example**

An example output is showing higher than normal CPU usage due to packets copied to the software forwarding task below:

```
console#show process cpu
Memory Utilization Report
```
status bytes
------- -------
free    1055653888
alloc   672153600

CPU Utilization:

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>5 Secs</th>
<th>60 Secs</th>
<th>300 Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1129</td>
<td>osapiTimer</td>
<td>0.09%</td>
<td>0.02%</td>
<td>0.01%</td>
</tr>
<tr>
<td>1137</td>
<td>bcmCNTR.0</td>
<td>0.19%</td>
<td>0.28%</td>
<td>0.30%</td>
</tr>
<tr>
<td>1142</td>
<td>bcmRX</td>
<td>18.00%</td>
<td>12.04%</td>
<td>11.10%</td>
</tr>
<tr>
<td>1155</td>
<td>bcmLINK.0</td>
<td>0.39%</td>
<td>0.37%</td>
<td>0.36%</td>
</tr>
<tr>
<td>1156</td>
<td>cpuUtilMonitorTask</td>
<td>0.09%</td>
<td>0.04%</td>
<td>0.04%</td>
</tr>
<tr>
<td>1170</td>
<td>nim_t</td>
<td>0.09%</td>
<td>0.07%</td>
<td>0.07%</td>
</tr>
<tr>
<td>1222</td>
<td>snoopTask</td>
<td>0.09%</td>
<td>0.02%</td>
<td>0.02%</td>
</tr>
<tr>
<td>1243</td>
<td>ipMapForwardingTask</td>
<td>27.30%</td>
<td>24.19%</td>
<td>29.06%</td>
</tr>
<tr>
<td>1257</td>
<td>tRtrDiscProcessingT</td>
<td>0.09%</td>
<td>0.01%</td>
<td>0.00%</td>
</tr>
<tr>
<td>1291</td>
<td>RMONTask</td>
<td>0.00%</td>
<td>0.02%</td>
<td>0.03%</td>
</tr>
<tr>
<td>1293</td>
<td>boxes Req</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.01%</td>
</tr>
</tbody>
</table>

Total CPU Utilization  55.91%  45.40%  48.02%

**show dos-control**

Use the `show dos-control` command to display Denial of Service configuration information.

**Syntax**

`show dos-control`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.
Example
The following example displays Denial of Service configuration information.

```
console#show dos-control
SIPDIP Mode...............................Disable
First Fragment Mode.......................Disable
Min TCP Hdr Size.........................20
TCP Fragment Mode ......................Disable
TCP Flag Mode..............................Disable
L4 Port Mode..............................Disable
ICMP Mode.................................Disable
Max ICMP Pkt Size.........................512
```

**show system internal pktmgr**

Use the `show system internal pktmgr` command to display the configured CPU rate limit for unknown packets in packets per second.

**Syntax**

`show system internal pktmgr internal control sw-rate-limit`

**Default Configuration**

This command has no default configuration.

**Command Modes**

Privileged Exec mode

**User Guidelines**

See the `rate-limit cpu` command for further information on the output of this command.

**Example**

```
console# show system internal pktmgr internal control sw-rate-limit
Inband pps global threshold 1024
```
storm-control broadcast

Use the `storm-control broadcast` command to enable broadcast storm recovery mode for a specific interface. Use the `no` form of the command to disable storm control or to return the configuration to the default.

**Syntax**

```
storm-control broadcast [{level level | rate rate | action {shutdown | trap}}]
no storm-control broadcast [level | rate | action]
```

- **level**— The configured rate as a percentage of link bandwidth (Range: 0-100)
- **rate** — The configured rate in packets per second. (Range: 0-14880000)
- **action shutdown**—Places the interface in the D-disable state if the threshold is exceeded.
- **action trap**—Logs a message and issue a trap if the threshold is exceeded.

**Default Configuration**

By default, broadcast storm control is disabled on all Ethernet interfaces. The default threshold for broadcast traffic is 5% of link bandwidth. The default behavior is to rate limit (drop) traffic exceeding the configured threshold. There is no default action.

**Command Mode**

Interface Configuration (Ethernet) mode, Interface Range mode

**User Guidelines**

Broadcast storm control can only be enabled on Ethernet interfaces. It cannot be configured on port channels. Setting the level, rate or action enables broadcast storm control. When enabled, broadcast storm control can issue a trap and drop traffic in excess of the configured rate (level) or shut down the port if the rate is exceeded. Either the level or the rate threshold may be configured, but not both.
Either the trap action or the shutdown action may be specified, but not both. The trap action issues a log message and a trap when the configured threshold is exceeded. Traffic exceeding the threshold is dropped.

The shutdown action shuts down the interface, puts the interface into the D-disable state, issues a log message (WARNING) and a trap. The operator may bring the port back into service using the no shutdown command.

Use the show storm-control action and show storm-control all commands to display the storm control settings.

Example
The following example configures any port to drop excess broadcast traffic and issue a log and trap if the received broadcast traffic exceeds 10% of link bandwidth:

```
console(config)#interface range gi1/0/1-24
console(config-if)#storm-control broadcast level 10
console(config-if)#storm-control broadcast action trap
console(config-if)#exit
```

storm-control multicast

Use the storm-control multicast command in Interface Configuration mode to enable multicast storm storm control for an interface.

Use the no form of the command to disable storm-control in order to return the configuration to the default.

Syntax

```
storm-control multicast [level level | rate rate | action {shutdown | trap}]
no storm-control multicast [level | rate | action]
```

- **level**— The configured rate as a percentage of link-speed.
- **rate**— The configured rate in packets per second. (Range: 0-14880000)
- **action shutdown**—Places the interface in the D-disable state if the threshold is exceeded.
- **action trap**—Logs a message and issue a trap if the threshold is exceeded.
**Default Configuration**

By default, multicast storm control is not enabled on any interfaces. The default threshold for multicast traffic is 5% of link bandwidth. The default behavior is to rate limit (drop) traffic exceeding the configured threshold. The default action is no action.

**Command Mode**

Interface Configuration (Ethernet) mode, Interface Range mode

**User Guidelines**

Multicast storm control applies to unknown multicast (i.e., multicast groups that are not control plane traffic and are not currently active on any interface). This is multicast traffic that normally is flooded in the VLAN. Multicast storm control can issue a trap and drop traffic in excess of the configured rate (level), or shut down the ingress port if the rate is exceeded. Multicast storm control can only be enabled on Ethernet interfaces. It cannot be configured on port channels.

Setting the level, rate or action does not enable multicast storm control. Issue the `storm-control multicast` command separately to enable multicast storm control.

Either the level or the rate threshold may be configured, but not both.

Either the trap action or the shutdown action may be specified, but not both.

The `trap` action issues a log message (WARNING) and a trap when the configured threshold is exceeded. Traffic exceeding the threshold is dropped.

The `shutdown` action shuts down the interface, puts the interface into the D-disable state, issues a log message and a trap. The operator may bring the port back into service using the `no shutdown` command.

Use the `show storm-control action` and `show storm-control all` commands to display the storm control settings.

**Example**

The following example configures any port to shut down if the received multicast traffic rate exceeds 20% of link bandwidth:
console(config)#interface range gi1/0/1-24
console(config-if)#storm-control multicast level 20
console(config-if)#storm-control multicast action shutdown
console(config-if)#exit

**storm-control unicast**

Use the `storm-control unicast` command in Interface Configuration mode to enable storm control for an interface. Unicast storm control limits the number of unicast destination lookup failures (DLFs). Use the `no` form of the command to disable unicast storm control or to return the configuration to the default.

**Syntax**

```
storm-control unicast [level level | rate rate | action{shutdown | trap}]
no storm-control unicast [level | rate]
```

- **level**—The configured rate as a percentage of link bandwidth (Range: 0-100)
- **rate**—The configured rate in packets per second. (Range: 0-14880000)
- **action**—The configured action: shutdown or trap.

**Default Configuration**

By default, unicast storm control is not enabled on any interfaces. The default threshold for unicast traffic is 5% of link bandwidth.

**Command Mode**

Interface Configuration (Ethernet) mode, Interface Range mode

**User Guidelines**

A destination lookup failure (DLF) is when a L2 unicast packet is unable to resolve the destination MAC address to an egress interface (no MAC forwarding address entry exists). The standard behavior for L2 DLFs is to flood the packet on all ports in the VLAN other than the port on which the packet was received. This flooding behavior can cause significant amounts of bandwidth to be consumed, potentially disrupting the forwarding of other traffic.
Unicast storm control can issue a trap and drop packets in excess of the configured rate (level) or shut down the port when the rate is exceeded. Setting the level, rate or action enables storm control. The shutdown action disables the interface when a packet storm is detected. The trap action issues an SNMP trap to configured SNMP agents.

Unicast storm control can only be enabled on Ethernet interfaces. It cannot be configured on port channels.

Either the level or the rate threshold may be configured, but not both.

Use the `show storm-control action` and `show storm-control all` commands to display the storm control settings.

**Example**

The following example configures any port to rate limit DLF traffic rate to 5% of link bandwidth:

```
console(config)#interface range gi1/0/1-24
console(config-if)#storm-control unicast level 5
console(config-if)#exit
```
In order to ensure the security of the switch management features, the administrator may elect to configure a management access control list. The Management Access Control and Administration List (ACAL) component is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP. Management ACLs are only configurable on IP (in-band) interfaces, not on the out-of-band interface or the serial port, and only filter packets sent to the switch CPU. Packets that are forwarded by the switch are not filtered by Management ACLs. Management ACLs filter packets in firmware after all hardware based ACLs (ip access-list and ipv6 access-list) have been applied. This allows the administrator to configure hardware based filtering criteria for in-band management access and then further refine that criteria with firmware based filtering supplied by the management ACL capability.

When a Management ACAL is enabled, incoming TCP packets initiating a connection (TCP SYN) and UDP packets will be filtered based on their source IP address and destination port. Additionally, other attributes such as incoming port (or port-channel) and VLAN ID can be used to determine if the traffic should be allowed access to the management interface. When the Management Access Control component is disabled, incoming TCP/UDP packets are not filtered in firmware and are processed normally. TCP SYN packets or UDP packets addressed to the following destination port numbers are not processed by the management ACL list: DNS(53), DHCP Server(67), DHCP Client (68), TFTP(69), telnet(23), HTTP(80), HTTPS(443), SNMP(161), SSH(22), and JAVA(4242).

There is also an option to restrict all the above packets from the network interface. This is done by specifying “console only” in the MACAL component. If this option is enabled, the system management interface is only accessible via the serial port. All TCP SYN packets and UDP packets are dropped except UDP packets sent to the ports listed above.

**Commands in this Section**

This section explains the following commands:
**deny (management)**

Use the `deny` command in Management Access-List Configuration mode to set conditions for disallowing packets to flow to the switch management function.

**Syntax**

```plaintext
deny [gigabitethernet unit/slot/port | vlan vlan-id | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port] [service service] [priority priority]
deny ip-source ip-address [mask mask | prefix-length] [gigabitethernet unit/slot/port | vlan vlan-id | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port] [service service] [priority priority]
```

- `gigabitethernet unit/slot/port` — A valid 1-Gigabit Ethernet-routed port number.
- `vlan vlan-id` — A valid VLAN number.
- `port-channel port-channel-number` — A valid routed port-channel number.
- `tengigabitethernet unit/slot/port` — A valid 10-Gigabit Ethernet-routed port number.
- `fortygigabitethernet unit/slot/port` — A valid 40-Gigabit Ethernet-routed port number.
- `ip-address` — Source IP address.
- `mask mask` — Specifies the network mask of the source IP address.
- `mask prefix-length` — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
• **service** service — Indicates service type. Can be one of the following: telnet, ssh, http, https, tftp, snmp, sntp, or any. The any keyword indicates that the service match for the ACL is effectively “don’t care”.

• **priority** priority — Priority for the rule. (Range: 1–64)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Management Access-list Configuration mode

**User Guidelines**

Rules with gigabitethernet, tengigabitethernet, fortygigabitethernet, vlan, and port-channel parameters are valid only if an IP address is defined on the appropriate interface. Ensure that each rule has a unique priority.

**Example**

The following example shows how all ports are denied in the access-list called mlist.

```
console(config)# management access-list mlist
console(config-macal)# deny
```

**management access-class**

Use the management access-class command in Global Configuration mode to restrict switch management connections. To disable any restrictions, use the no form of this command.

**Syntax**

```
management access-class {console-only | name}
no management access-class
```

- **name** — A valid access-list name. (Range: 1–32 characters)
- **console-only** — The switch can be managed only from the console.
**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
The active management access-list processes IPv4 TCP/UDP packets only. Packets for certain management protocols are allowed to pass to the CPU without processing by the management ACL list. Specifically, TCP or UDP packets addressed to the following destination port numbers are not processed by the management ACL list: DNS(53), DHCP Server(67), DHCP Client (68), TFTP(69), telnet(23), HTTP(80), HTTPS(443), SNMP(161), SSH(22), and JAVA(4242). A rate-limiting egress CPU ACL would be ideal to mitigate smurf style attacks on these ports.

Only a single management access list can be active at a time. However, it can have multiple permit/deny conditions.

**Example**
The following example configures an access-list called mlist as the management access-list.

```
console(config)# management access-list mlist
```

**management access-list**
Use the `management access-list` command in Global Configuration mode to define an access list for management, and enter the access-list configuration mode for editing the access list conditions. Once in access-list configuration mode, access conditions are configured with the `deny` and `permit` commands. To remove an access list, use the `no` form of this command.

**Syntax**

```
management access-list name
no management access-list name
```

- `name` — The access list name. (Range: 1–32 printable characters)
**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

A management access list is only supported on the switched interfaces. It is not supported on the out-of-band interface.

This command enters the access-list configuration mode, where access conditions may be defined with **deny** and **permit** commands.

If no match criteria are defined the default is to **deny** the packet (i.e., the packet is dropped).

If editing an access-list context, new rules are appended to the end of the access-list.

Use the **management access-class** command to select the active access-list.

The active management list cannot be updated or removed.

Management access list names can consist of any printable character, including blanks. Enclose the name in quotes to embed blanks in the name. Question marks are disallowed.

**Examples**

The following example shows how to permit access to switch management via two Ethernet interfaces, Gigabit Ethernet 1/0/1 and Gigabit Ethernet 1/0/9.

```plaintext
console(config)#management access-list mlist
console(config-macal)# permit gigabitethernet 1/0/1 priority 1
console(config-macal)# permit gigabitethernet 1/0/9 priority 1
console(config-macal)# exit
console(config)#management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Gigabit Ethernet 1/0/1 and Gigabit Ethernet 1/0/9.

```plaintext
console(config)# management access-list mlist
console(config-macal)# deny gigabitethernet 1/0/1 priority 1
console(config-macal)# deny gigabitethernet 1/0/9 priority 2
console(config-macal)# permit priority 2
```
no priority (management)

Use the `no priority` command to remove a permit or deny condition from a Management Access list.

**Syntax**

```plaintext
no priority priority
```

- `priority-value`—The priority of the permit or deny rule to be removed. The range is 1 to 64.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Management Access-list Configuration mode

**User Guidelines**

A rule with the specified priority-value must exist in order to be removed.

**Command History**

Command introduced in version 6.5 firmware.

permit (management)

Use the `permit` command in Management Access-List configuration mode to set conditions for allowing packets to flow to the switch management function.

**Syntax**

```plaintext
permit ip-source ip-address [mask mask | prefix-length] [gigabitethernet unit/slot/port | vlan vlan-id | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port] [service service] [priority priority-value]
```
permit {gigabitethernet unit/slot/port | vlan vlan-id | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port} [service service] [priority priority-value]

**permit service** service [priority priority-value]

**permit priority** priority-value

- **gigabitethernet** unit/slot/port — A valid Gigabit Ethernet routed port number.
- **vlan** vlan-id — A valid VLAN number.
- **port-channel** port-channel-number — A valid port channel number.
- **tengigabitethernet** unit/slot/port — A valid 10-Gigabit Ethernet routed port number.
- **fortygigabitethernet** unit/slot/port — A valid 40-Gigabit Ethernet routed port number.
- **ip-address** — Source IP address.
- **mask** mask — Specifies the network mask of the source IP address.
- **mask** prefix-length — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **service** service — Indicates service type. It can be one of the following: **telnet**, **ssh**, **http**, **https**, **tftp**, **snmp**, **sntp**, or **any**. The **any** keyword indicates that the service match for the ACL is effectively “don’t care”.
- **priority** priority-value — Priority for the rule. (Range: 1 – 64)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Management Access-list Configuration mode

**User Guidelines**

Rules with **gigabitethernet**, **tengigabitethernet**, **fortygigabitethernet**, **vlan**, and **port-channel** parameters are valid only if an IP address is defined on the appropriate interface.
If the priority-value is not specified when inputting a rule, the system assigns the lowest numbered unused priority-value in the range 1–64. If a rule is input with an existing priority-value, the original rule is overwritten.

**Examples**

The following example shows how to allow global access for two management interfaces, Gigabit Ethernet 1/0/1 and Gigabit Ethernet 1/0/9.

```
console(config)#management access-list mlist
console(config-macal)# permit gigabitethernet 1/0/1 priority 1
console(config-macal)# permit gigabitethernet 1/0/9 priority 2
console(config-macal)# exit
console(config)# management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Gigabit Ethernet 1/0/1 and 1/0/9.

```
console(config)# management access-list mlist
console(config-macal)# deny gigabitethernet 1/0/1 priority 1
console(config-macal)# deny gigabitethernet 1/0/9 priority 2
console(config-macal)# permit priority 3
console(config-macal)# exit
console(config)# management access-class mlist
```

**show management access-class**

Use the `show management access-class` command to display information about the active management access list.

**Syntax**

`show management access-class`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the management access-list information.

```console
console# show management access-class
Management access-class is enabled, using access list mlist
```

**show management access-list**

Use the `show management access-list` command to display management access-lists.

**Syntax**

```
show management access-list [name]
```

- name — A valid access list name. (Range: 1–32 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the active management access-list.

```console
console# show management access-list
mlist
-----
permit priority 1 gigabitethernet 1/0/1
permit priority 2 gigabitethernet 2/0/1
! (Note: all other access implicitly denied)
```
Password Management Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Password Management component supports configuration of strength checks intended to ensure that network operators utilize passwords that are difficult to crack. In addition, the administrator can age passwords, ensure that operators do not reuse passwords, and lock out operator accounts when multiple attempts to enter incorrect passwords are detected. Passwords are masked from view when entered by the user and in the running config.

**Configurable Minimum Password Length**

The administrator has the option of requiring user passwords to be a minimum length. The administrator can choose to have the switch enforce a minimum length between 8 and 64 characters. The default minimum length is 8 although there is no default password (zero length string).

**Password History**

Keeping a history of previous passwords ensures that users cannot reuse passwords often. The administrator can configure the switch to store up to 10 of the last passwords for each user. The default operation is that no history is stored.

**Password Aging**

The switch can implement an aging process on passwords and require users to change them when they expire. The administrator can configure the switch to force a password change between 1 and 365 days. By default, password aging is disabled. When a password expires, the user must enter a new password before continuing.

**User Lockout**

The administrator may choose to strengthen the security of the switch by enabling the user lockout feature. A lockout count between 1 and 5 attempts can be configured. When a lockout count is configured, then a user that is
logging in must enter the correct password within that count. Otherwise, that user is locked out from further remote switch access. Only an administrator with read/write access can reactivate that user. The user lockout feature is disabled by default. The user lockout feature applies to all users on all ports. The administrator can access the serial port even if he/she is locked out and reset the password or clear the config to regain control of the switch. This ensures that if a hacker tries to log in as admin and causes the account to be locked out, then the administrator with physical access to the switch can still log in and reactivate the admin account.

**Password Strength**

Password Strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. The strength of a password is a function of length, complexity and randomness. Using strong passwords lowers overall risk of a security breach. The scope of this feature is to enforce a baseline Password Strength for all locally administered users.

The feature doesn’t affect users with an existing password until their password ages out. Password Strength is only enforced when a user is configuring a new password or changing their existing password. The default action is Disabled in FP and is independent of any platform. The network operator has to take care that the Password Strength check is Disabled before downloading scripts containing old users to avoid password configuration failure for such users.

**Password Strength Definition:**

The feature ensures that any password configured on the switch for local administration purpose is a strong password and conforms to each of the following characteristics when configured:

- Minimum number of uppercase letters.
- Minimum number of lowercase letters.
- Minimum number of numeric characters.
- Minimum number of special characters from the set: `! "$ '? % ^ & * ( ) _ - + = \{ \[ \} ; : @ ' ~ # | \< , > . ? /.
- Does not contain the associated login name.
- Maximum number of consecutive characters (such as abcd).
• Maximum number of consecutive numbers (such as 1234).
• Maximum number of repetition of characters or numbers (such as 1111 or aaaa).

Configuring minimum value of 0 for the above parameters means no restriction on that set of characters and configuring maximum of 0 means disabling the restriction (or no limit on the maximum number of course limited by minimum password length). Implicitly, configuring a minimum value of 0 means a user may enter a valid password consisting entirely of those characters unless minimum character class checking is also enabled with some non-zero minimum strength check values.

The Password strength feature applies to all login passwords (user, line and enable).

**Commands in this Section**

This section explains the following commands for viewing and configuring properties of passwords:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwords aging</td>
<td>passwords strength minimum special-characters</td>
</tr>
<tr>
<td>passwords history</td>
<td>passwords strength max-limit consecutive-characters</td>
</tr>
<tr>
<td>passwords lock-out</td>
<td>passwords strength max-limit repeated-characters</td>
</tr>
<tr>
<td>passwords min-length</td>
<td>passwords strength minimum character-classes</td>
</tr>
<tr>
<td>passwords strength-check</td>
<td>passwords strength exclude-keyword</td>
</tr>
<tr>
<td>passwords strength minimum uppercase-letters</td>
<td>enable password encrypted</td>
</tr>
<tr>
<td>passwords strength minimum lowercase-letters</td>
<td>show passwords configuration</td>
</tr>
<tr>
<td>passwords strength minimum numeric-characters</td>
<td>show passwords result</td>
</tr>
</tbody>
</table>

**NOTE:** To change a password, use the **passwords** command, which is described in **AAA Commands**.
passwords aging

Use the passwords aging command in Global Configuration mode to implement aging on passwords for local users. When a user’s password expires, the user is prompted to change it before logging in again. Use the no form of this command to set the password aging to the default value.

Syntax
passwords aging 1-365
no passwords aging

Default Configuration
The default value is 0.

Command Mode
Global Configuration mode

User Guidelines
A value of 0 days disables password aging. Password aging uses the time-of-day clock, therefore having an accurate clock source is required. The use on SNTP is strongly recommended.

Example
The following example sets the password age limit to 100 days.

console(config)#passwords aging 100

passwords history

As administrator, use the passwords history command in Global Configuration mode to set the number of previous passwords that are stored for each user account. When a local user changes his or her password, the user is not able to reuse any password stored in password history. This setting ensures that users do not reuse their passwords often. The default is 0. Use the no form of this command to set the password history to the default value of 0.
**Syntax**

passwords history 0-10
no passwords history

**Default Configuration**
The default value is 0.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets the number of previous passwords remembered by the system at 10.

```
console(config)#passwords history 10
```

**passwords lock-out**

Use the `passwords lock-out` command in Global Configuration mode to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user who is logging in must enter the correct password within that count. Otherwise that user is locked out from further switch access. Only a user with read/write access can reactivate a locked user account. Password lockout does not apply to logins from the serial console. Use the `no` form of this command to set the password lockout count to the default value.

**Syntax**

passwords lock-out 1-5
no passwords lock-out

**Default Configuration**
The default value is 0 or no lockout count is enforced.
**Command Mode**
Global Configuration mode.

**User Guidelines**
Password lockout only applies to users with authentication configured to local. RADIUS or TACACS authenticated users will use policies configured on the respective RADIUS/TACACS servers.

**Example**
The following example sets the number of user attempts before lockout at 2.
```
console(config)#passwords lock-out 2
```

**passwords min-length**
Use the **passwords min-length** command in Global Configuration mode to enforce a minimum length password length for local users. The value also applies to the **enable** password. The valid range is 8–64. The default is 8. Use the **no** version of this command to set the minimum password length to 8.

**Syntax**
```
passwords min-length length
no passwords min-length
```

- **length** — The minimum length of the password (Range: 8–64 characters)

**Default Configuration**
By default, the minimum password length is 8 characters.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.
Example
The following example configures user **bob** with password **xxyyymmmm** and user level 15.

```
(config)# username bob password xxyyymmmm privilege 15
```

**passwords strength-check**

Use the **passwords strength-check** command in Global Configuration mode to enable the Password Strength feature. The command is used to enable the checking of password strength during user configuration. Use the **no** form of the command to disable the Password Strength feature.

**Syntax**

```
passwords strength-check
don passwords strength-check
```

**Default Configuration**

The password strength feature is disabled by default.

**Command Mode**

Global Configuration

**User Guidelines**

This command enables/disables enforcement of password strength checking policy as configured by the following commands:

- **passwords strength minimum uppercase-letters**
- **passwords strength minimum lowercase-letters**
- **passwords strength minimum special-characters**
- **passwords strength minimum numeric-characters**
- **passwords strength max-limit consecutive-characters**
- **passwords strength max-limit repeated-characters**
- **passwords strength minimum character-classes**

Minimum strength validation validates a password containing a character in the corresponding character class. If a character class is configured with a strength check minimum of 0 (the default), a user may enter a valid password containing only characters from that class and pass the strength check. Therefore, it is recommended that the administrator configure all four
minimum strength check character classes if password strength checking is desired. Use the minimum character class check to require the user to enter a password that passes the minimum strength check for more than one minimum strength check character class.

Minimum character class checking validates passwords that contain a character matching a configured character class. If minimum character class checking is enabled, a password must pass at least the minimum number of configured minimum strength class checks to be valid. Non-configured minimum character classes are not counted towards the minimum matching character classes.

If minimum character class checking is disabled and if a password contains a character matching a configured character class, it must meet the specific minimum strength check limit for the matching character class. If the password only contains characters that are in non-configured (0 limit) minimum strength check character class, the password is considered valid.

If the maximum consecutive characters or maximum repeated characters limits, or other validation checks are configured, passwords must pass these tests regardless of the minimum character class checking setting.

**passwords strength minimum uppercase-letters**

Use this command to enforce a minimum number of uppercase letters that a password must contain. The valid range is 0–16. The default is 1. A minimum of 0 means no restriction on that set of characters. Use the no form of the command to reset the minimum uppercase letters to the default value.

**Syntax**

```
passwords strength minimum uppercase-letters 0–16
no passwords strength minimum uppercase-letters
```

**Default Configuration**

The default value is 1.

**Command Mode**

Global Configuration
**User Guidelines**

This limit is not enforced unless the `passwords strength minimum uppercase-letters` command is configured with a value greater than 0. In other words, with a configuration of 0, a password consisting entirely of upper case letters will pass the minimum strength check criteria.

**Example**

```
console(config)#passwords strength minimum uppercase-letters 6
```

**passwords strength minimum lowercase-letters**

Use this command to enforce a minimum number of lowercase letters that a password must contain. The valid range is 0–16. The default is 1. A setting of 0 means no restriction. Use the `no` form of this command to reset the minimum lowercase letters to the default value.

**Syntax**

```
passwords strength minimum lowercase-letters 0–16
no passwords strength minimum lowercase-letters
```

**Default Configuration**

The default value is 1.

**Command Mode**

Global Configuration

**User Guidelines**

This limit is not enforced unless the `passwords strength minimum lowercase-letters` command is configured with a value greater than 0. In other words, a password consisting entirely of lower case letters will pass the minimum strength check criteria.

**Example**

```
console(config)#passwords strength minimum lowercase-letters 6
```
**passwords strength minimum numeric-characters**

Use this command to enforce a minimum number of numeric numbers that a password should contain. The valid range is 0–16. The default is 1. A minimum of 0 means no restriction on that set of characters. Use the no form of this command to reset the minimum numeric characters to the default value.

**Syntax**

passwords strength minimum numeric-characters 0–16
no passwords strength minimum numeric-characters

**Default Configuration**

The default value is 1.

**Command Mode**

Global Configuration

**User Guidelines**

This limit is not enforced unless the passwords strength minimum numeric-characters command is configured with a value greater than 0. In other words, a configuration of 0 allows a password consisting entirely of numeric characters to pass strength check validation.

**Example**

```
console(config)#passwords strength minimum numeric-characters 6
```

**passwords strength minimum special-characters**

Use this command to enforce a minimum number of special characters that a password may contain. The valid range is 0–16. The default is 1. A setting of 0 means no restriction. Special characters are one of the following characters (\`! $ % ^ & * ( ) _ - + = { [ ] } : ; @ ~ # | \< , > ./) Use the no form of this command to reset the minimum special characters to the default value.
**Syntax**

passwords strength minimum special-characters 0–16
no passwords strength minimum special-characters

**Default Configuration**

The default value is 1.

**Command Mode**

Global Configuration

**User Guidelines**

This limit is not enforced unless the passwords strength minimum special-characters command is configured with a value greater than 0. In other words, a configuration of 0 allows a password consisting entirely of special characters to pass strength check validation.

**Example**

console(config)#passwords strength minimum special-characters 6

**passwords strength max-limit consecutive-characters**

Use this command to enforce a maximum number of consecutive characters that a password can contain. If a user enters a password that has more consecutive characters than the configured limit, the system rejects the password. The valid range of consecutive characters is 0–15. The default is 0. A maximum of 0 means there is no restriction on consecutive characters. Examples of consecutive characters are ABCDEF or 123456 or !"#$%&’(). Use the no form of this command to reset the maximum consecutive characters accepted to the default value.

**Syntax**

passwords strength max-limit consecutive-characters 0–15
no passwords strength max-limit consecutive-characters
**Default Configuration**
The default value is 0.

**Command Mode**
Global Configuration

**User Guidelines**
This command has no user guidelines.

**Example**
console(config)#passwords strength max-limit consecutive-characters 3

**passwords strength max-limit repeated-characters**

Use this command to enforce a maximum repeated characters that a password should contain. If password has repetition of characters more than the configured max-limit, it fails to configure. The valid range is 0-15. The default is 0. A maximum of 0 means again disabling the restriction. Use the no form of this command to reset the maximum repeated characters to the default value.

**Syntax**
passwords strength max-limit repeated-characters 0-15
do passwords strength max-limit repeated-characters

**Default Configuration**
The default value is 0.

**Command Mode**
Global Configuration

**User Guidelines**
This command has no user guidelines.
Example

console(config)# passwords strength max-limit repeated-characters 3

passwords strength minimum character-classes

Use this command to enforce a minimum number of character classes that a password must contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 0. If a value of 0 is configured then no character class checking is performed, i.e. the password need not contain characters from more than one character class. Configured minimum strength and maximum strength checking is still performed for each individual character class, if configured. Use the no form of this command to reset the minimum character-classes to the default value.

Syntax

passwords strength minimum character-classes 0-4
no passwords strength minimum character-classes

Default Configuration

The default value is 0. This character class limit is not enforced unless the passwords strength minimum character-classes command is configured with a value greater than 0.

Command Mode

Global Configuration

User Guidelines

This command is used to enable password character class checking using the parameters set by the following commands:

- passwords strength minimum uppercase-letters
- passwords strength minimum lowercase-letters
- passwords strength minimum special-characters
- passwords strength minimum numeric-characters
A value greater than 0 specifies the minimum number of character class tests a password must contain. A value of 0 disables checking that the password contains characters from the requisite number of character classes. Minimum character class checking validates passwords that contain at least one character matching a character class. If minimum character class checking is enabled, a password must contain at least one character from a minimum number of character classes to be valid.

Even if the minimum character class checking is disabled, passwords containing characters from a class must still meet the specific minimum strength limit for the matching class. If the password only contains characters from non-configured character classes, the password is considered valid.

If the maximum consecutive characters or maximum repeated characters limits are configured, passwords must pass these tests regardless of the minimum character class checking setting.

**Example**

console(config)#passwords strength minimum character-classes 4

**passwords strength exclude-keyword**

Use this command to exclude the keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case insensitive and reverse) as a substring. You can configure up to a maximum of three keywords. Use the `no` form of this command to reset the restriction for a given string or all the strings configured.

**Syntax**

passwords strength exclude-keyword string

no passwords strength exclude-keyword [string]

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration
**User Guidelines**
This command has no user guidelines.

**Example**
```plaintext
console(config)#passwords strength exclude-keyword dell
```

**enable password encrypted**
This command is used by an Administrator to transfer the enable password between devices without having to know the password.

**Syntax**
enable password password encrypted

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
The password parameter must be exactly 128 hexadecimal characters.

**show passwords configuration**
Use the `show passwords configuration` command to display the configured password management settings.

**Syntax**
show passwords configuration

**Default Configuration**
This command has no default configuration.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following fields are displayed by this command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td>Minimum number of characters required when changing passwords.</td>
</tr>
<tr>
<td>Password History</td>
<td>Number of passwords to store for reuse prevention.</td>
</tr>
<tr>
<td>Password Aging</td>
<td>Length in days that a password is valid.</td>
</tr>
<tr>
<td>Lockout Attempts</td>
<td>Number of failed password login attempts before lockout.</td>
</tr>
<tr>
<td>Minimum Password Uppercase Letters</td>
<td>Minimum number of uppercase characters required when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Lowercase Letters</td>
<td>Minimum number of uppercase characters required when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Numeric Characters</td>
<td>Minimum number of numeric characters required when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Special Characters</td>
<td>Minimum number of special characters required when configuring passwords.</td>
</tr>
<tr>
<td>Maximum Password Consecutive Characters</td>
<td>Maximum number of consecutive characters required that the password should contain when configuring passwords.</td>
</tr>
<tr>
<td>Maximum Password Repeated Characters</td>
<td>Maximum number of repetition of characters that the password should contain when configuring passwords.</td>
</tr>
</tbody>
</table>
Example

The following example displays the command output.

```console
console#show passwords configuration
Passwords Configuration
----------------------------------------
Minimum Password Length.................... 8
Password History............................ 0
Password Aging (days)........................ 0
Lockout Attempts............................ 0
Password Strength Check.................... Enable
Minimum Password Uppercase Letters........... 4
Minimum Password Lowercase Letters.......... 4
Minimum Password Numeric Characters........ 3
Minimum Password Special Characters........ 3
Maximum Password Consecutive Characters..... 3
Maximum Password Repeated Characters....... 3
Minimum Password Character Classes.......... 4
Password Exclude Keywords................... dell, dell1, dell2
```

**show passwords result**

Use the `show passwords result` command to display the last password set result information.

**Syntax**

`show passwords result`

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the command output.

```
console#show passwords result
Last User whose password is set....................... dell
Password strength check............................ Enable
Last Password Set Result:
Reason for failure: Could not set user password! Password should contain at least 4 uppercase letters.
```
SSH Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Management access to the switch is supported via telnet, SSH, or the serial console. The Dell EMC Networking supports secure shell (SSH) and secure sockets layer (SSL) to help ensure the security of network transactions.

Keys and certificates can be generated externally (that is, offline) and downloaded to the target or generated directly by the Dell EMC Networking switch.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate dsa</td>
<td>For generating DSA key pairs for the SSH server.</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>crypto key pubkey-chain ssh</td>
<td></td>
</tr>
<tr>
<td>crypto key zeroize pubkey-chain</td>
<td></td>
</tr>
<tr>
<td>crypto key zeroize {rsa</td>
<td>dsa}</td>
</tr>
<tr>
<td>ip ssh port</td>
<td></td>
</tr>
</tbody>
</table>

**crypto key generate dsa**

Use the `crypto key generate dsa` command in Global Configuration mode to generate DSA key pairs for the SSH server. A key pair is one public DSA key and one private DSA key. Use the `crypto key zeroize` command to remove the generated private key from the local file system. The public and private keys will be overwritten if the command is subsequently executed.

**Syntax**

crypto key generate dsa

**Default Configuration**

DSA key pairs do not exist.
**Command Mode**

Global Configuration mode

**User Guidelines**

DSA keys are generated in pairs: one public DSA key and one private DSA key. These keys are used the encrypt communication with the switch when using SSH or HTTPS. If your switch already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys. Existing certificates generated from the previous keys will be invalidated. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. DSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Use the `crypto key zeroize dsa` command to remove the DSA key pair from the system.

Private keys should never be shared with unauthorized users. This command generates the following private/public key pair in the `ssh_host_dsa_key` and `ssh_host_dsa_key.pub` files. Both the RSA and DSA keys must be generated to enable the SSH server.

**Example**

The following example generates DSA key pairs.

```
console(config)#crypto key generate dsa
```

**crypto key generate rsa**

Use the `crypto key generate rsa` command in Global Configuration mode to generate RSA key pairs for use by the SSH or HTTPS server. Use the `crypto key zeroize` form of the command to delete the private key from the local file system.

**Syntax**

`crypto key generate rsa`

**Default Configuration**

RSA key pairs do not exist.
**Command Mode**
Global Configuration mode

**User Guidelines**
RSA keys are generated in pairs: one public RSA key and one private RSA key. These keys are used to encrypt communication with the switch when using SSH. If your switch already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. RSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Use the `crypto key zeroize rsa` command to remove RSA key pair from the system.

Private keys should never be shared with unauthorized users. This command generates the private public key pairs in the following files: `ssh_host_rsa_key` and `ssh_host_rsa_key.pub`, `ssh_host_key` and `ssh_host_key.pub` files. Both the RSA and DSA keys must be generated to enable the SSH server.

**Example**
The following example generates RSA key pairs.

```
console(config)#crypto key generate rsa
```

**crypto key pubkey-chain ssh**
Use the `crypto key pubkey-chain ssh` command in Global Configuration mode to enter public key configuration mode in order to manually specify public keys for SSH clients or an individual user.

**Syntax**
```
crypto key pubkey-chain ssh user-key username rsa/dsa
```

**Default Configuration**
By default, this command has no public keys configured.
**Command Mode**
Global Configuration mode

**User Guidelines**
This public key is used to authenticate an administrator to the switch when using SSH. This avoids the need for the administrator to enter a password on every login.

Enclose the key string is quotes. The Key String is the contents of the public key in uu-encoded format.

**Example**
The following example configures a public key for administrator bob, enables the SSH server, and enables public key authentication over SSH.

```console
console#configure
cfg cle nocrypt key generate rsa
cfg cle nocrypt key generate dsa
cfg cle nocrypt key pubkey-chain ssh user-key bob rsa
Key-string row AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WHtjQDUygjSQXHVgyqdUby
Key-string row dxUXEAIuDHXcWHRvBr/ak1HDQitBzeEv1vVETOEn5ddLmRhtIGRdKUJHgBHJ
Key-string row R2VaSN/WC0IK53j9re4B11AE+03qAxwJs0KD7cTkvF9I+YdiXeOM8VE4skkw
Key-string row AiyLDNWXgNQ6iat8+8Mjth+PIo5t3HykYUCKd8B1v939z3i/sr4hHHJCdxw
Key-string row wRW3QtgXaGwYt2rd1r3x8ViAF6B7AKYd6xGvVjyjTD6TjrcRwHqB/BHsFr
Key-string row z/R11SYa0vFjel/7/0qADSHfHqWVajYKma4xP0tIye7oqzA0m1b7618uTB
Key-string row luBEoLQ+FKOMKi8sQ==
cfg cle nocrypt-pubkey-key#exit
cfg cle nocrypt #ip ssh server
cfg cle nocrypt #ip ssh pubkey-auth
```

**crypto key zeroize pubkey-chain**
Use the `crypto key zeroize pubkey-chain` command in Global Configuration mode to erase all SSH server public key chains or the public key chain for a user.

**Syntax**
`crypto key zeroize pubkey-chain ssh [user-key username]`
Default Configuration
There is no default configuration for this command.

Command Mode
Global Configuration mode.

User Guidelines
The SSH server requires the public and private keys RSA/DSA keys to operate.

Example
console(config)#crypto key zeroize pubkey-chain ssh user-key bob

crypto key zeroize {rsa|dsa}
Use the crypto key zeroize {rsa|dsa} command in Global Configuration mode to delete the RSA or DSA public and private keys from the switch.

Syntax
crypto key zeroize {rsa|dsa}

Default Configuration
There is no default configuration for this command.

Command Mode
Global Configuration mode.

User Guidelines
The crypto key zeroize rsa command removes the following files:
ssh_host_key
ssh_host_rsa_key
ssh_host_key.pub
ssh_host_rsa_key.pub
The `crypto key zeroize dsa` command removes the following files:

- `ssh_host_dsa_key`
- `ssh_host_dsa_key.pub`

Removing the keys does not terminate existing SSH sessions.

**Example**

```
console(config)#crypto key zeroize rsa
```

**ip ssh port**

Use the `ip ssh port` command in Global Configuration mode to specify the TCP port to be used by the SSH server. To use the default port, use the `no` form of this command.

**Syntax**

```
ip ssh port port-number
no ip ssh port
```

- `port-number` — Port number for use by the SSH server. (Range: 1025–65535)

**Default Configuration**

The default value is 22.

**Command Mode**

Global Configuration mode

**User Guidelines**

The SSH TCP port should not be set to a value that might conflict with other well-known protocol port numbers used on this switch. The following non-exhaustive list of ports are reserved to the system and may not be able to be configured for another purpose: 23 (telnet), 80 (HTTP), 161,162 (SNMP), 514, (SYSLOG), 546,547 (DHCPv6), 2222 (SSH).
Example
The following example specifies the port to be used by the SSH server as 8080.

```console
console(config)#ip ssh port 8080
```

**ip ssh pubkey-auth**

Use the `ip ssh pubkey-auth` command in Global Configuration mode to enable public key authentication for incoming SSH sessions. To disable this function, use the `no` form of this command.

**Syntax**

```
ip ssh pubkey-auth
no ip ssh pubkey-auth
```

**Default Configuration**

The function is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Public key authentication allow administrators with an SSH client access to the switch without requiring a password. Use the `crypto key pubkey-chain ssh user-key` command to configure the administrators public key for use by the SSH server. AAA authentication is independent from this configuration.

**Example**

The following example enables public key authentication for incoming SSH sessions.

```console
console(config)#ip ssh pubkey-auth
```
**ip ssh server**

Use the `ip ssh server` command in Global Configuration mode to enable the switch to be configured using SSH. To disable this function, use the `no` form of this command.

**Syntax**

```
ip ssh server
no ip ssh server
```

**Default Configuration**

The SSH server is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

To generate SSH server keys, use the commands `crypto key generate rsa` and `crypto key generate dsa` commands. These keys are required to allow the SSH server to operate.

Dell EMC Networking N-Series switches support the SSH service over IPv4 or IPv6. SSH is configured to require a password on accounts that attempt to log into the switch.

**Example**

The following example enables the switch to be configured using SSH.

```
console(config)#crypto key generate rsa
Do you want to overwrite the existing RSA keys? (y/n):y
RSA key generation started, this may take a few minutes...
RSA key generation complete.
console(config)#crypto key generate dsa
Do you want to overwrite the existing DSA keys? (y/n):y
DSA key generation started, this may take a few minutes...
DSA key generation complete.
console(config)#ip ssh server
```
key-string

Use the key-string SSH Public Key Configuration mode to specify an SSH public key manually.

Syntax

key-string key-string
key-string row key-string
  • row — To specify the SSH public key row by row.
  • key-string — The UU-encoded DER format is the same format as the authorized keys file used by OpenSSH.

Default Configuration

By default, the key-string is empty.

Command Mode

SSH Public Key Configuration mode

User Guidelines

The key string is the public key of the specified type (RSA or DSA) generated by the administrator. The administrator will need access to both the public and private key on the host to log in without authenticating via password. DSA is considered less secure than RSA. Use of RSA is recommended.

Use the key-string row command to enter the key-string one row at a time. The row may be enclosed in quotes. This command may be used to enter the key one line at a time should the key-string be greater than 234 characters in length.

Use the key-string command without the row parameter to enter the entire key at once if the key-string does not exceed 234 characters.

The switch accepts keys up to 2048 bits in length.

Command History

Modified in version 6.5 firmware.
Examples

The following example shows how to enter a single public key string for a user called “bob.”

```
console(config)#crypto key pubkey-chain ssh user-key bob rsa
Key-string row AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WHtjQDUygjSQQXHVgyqdUby
Key-string row dxUXEAIbDHXcWHVrOR/ak1HDQtBzeEv1vVEToEn5ddLmRhtIgRdKUJHgBHJv
Key-string row R2VaSN/WC0IK53j9re4B11AE+O3qAxwJs0KD7cTkvF9I+YdiXeOM8VE4skkw
Key-string row AiyLDNVWXgNQ6iat8+8Mjth+PIO5t3HyKYUCKd8B1v9nzi/sr4hHJHJd7w
Key-string row wRW3QtgXaGwYt2rd1r3x8ViAF6B7AKYd8xGVVjyJTD6TjrCRrwQHgB/BHsFr
Key-string row z/RlI7Ya0vFjel/7/0qaIDSHfHqWhajYkMa4xP0tIye7oqzA0mlb76l28uTB
Key-string row luBEoLQ+PKOKMiK8sQ==
```

show crypto key mypubkey

Use the show crypto key mypubkey command to display the SSH public keys of the switch.

Syntax

```
show crypto key mypubkey [rsa | dsa]
```

- rsa — RSA key.
- dsa — DSA key.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays the SSH public keys on the switch.

```
console#show crypto key mypubkey rsa
rsa key data:
    ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WHtjQDUygjSQQXHVgyqdUby
```
**show crypto key pubkey-chain ssh**

Use the `show crypto key pubkey-chain ssh` command to display SSH public keys stored on the switch.

**Syntax**

`show crypto key pubkey-chain ssh [username username] [fingerprint bubble-babble | hex]`

- **username** — Specifies the remote SSH client username. (Range: 1–48 characters)
- **bubble-babble** — Fingerprints in Bubble Babble format.
- **hex** — Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays all SSH public keys stored on the switch.

```
console#show crypto key pubkey-chain ssh
```
Username  Fingerprint
--------  -----------------------------------------------------------------

The following example displays the SSH public called “dana.”

```
console#show crypto key pubkey-chain ssh username dana
Username: dana
  rsa key data:
  ssh-rsa AAAAB3NzaC1yc2EAAAABIAwAAAIEAywqRKTRnexcxxVUVTeMl+Gkh
  imyUDhcTkgEfssLPMagoXITwzCE5+97U1IsSRKQQWR+pBNI45tCYd75LUofV
  4LP6Lj1Q5Q0w5lBiqC2MZ/iBHGSsHMAE0lYtel2prDu4uiZHMwWezmdQp9
  a1PU4jwQ22TlcfaUq3sqC3FMUoU=
```

**show ip ssh**

Use the `show ip ssh` command to display the SSH server configuration.

**Syntax**

```
show ip ssh
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the SSH server configuration.

```
console#show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:
  IP Address     User Name  Idle Time  SessionTime
```
| 10.240.1.122 | John     | 00:00:00 | 00:00:08 |
# Audio Visual Bridging Commands

**Dell EMC Networking N4000 Series Switches**

This section of the document contains the following audio visual bridging commands:

<table>
<thead>
<tr>
<th>Multiple MAC Registration Protocol Commands</th>
<th>Multiple Stream Reservation Protocol Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple VLAN Registration Protocol Commands</td>
<td>802.1AS Timesync Commands</td>
</tr>
</tbody>
</table>
Multiple MAC Registration Protocol Commands

Dell EMC Networking N4000 Series Switches

This section covers commands related to Multiple MAC Registration Protocol (MMRP). MMRP is an implementation of IEEE 802.1ak. MMRP supports registration of MAC address/VLAN pairs in support of Audio-Visual Bridging.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear mmrp statistics</th>
<th>mmrp periodic state machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>mmrp</td>
<td>show mmrp</td>
</tr>
<tr>
<td>mmrp global</td>
<td>show mmrp statistics</td>
</tr>
</tbody>
</table>

**clear mmrp statistics**

This command clears the MMRP statistics for an interface or all interfaces.

**Syntax**

clear mmrp statistics [ interface-id | all ]

- All—Clear MMRP statistics for all interfaces
- interface-id—Clear statistics for the specified interface.

**Default Configuration**

This command has no defaults.

**Command Mode**

Privileged Exec
**User Guidelines**

MMRP is not compatible with the GMRP. Do NOT enable GMRP/GVRP on MMRP enabled switches.

The `clear counters` command also clears all MMRP statistics for all interfaces in addition to clearing other counters.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example clears the MMRP counters on port channel 1

```
console#clear mmrp statistics po1
```

**mmrp**

This command enables MMRP on a specific interface. Use the `no` form of the command to disable MMRP on an interface.

**Syntax**

```
mmrp
no mmrp
```

**Default Configuration**

By default, MMRP is disabled globally and on all interfaces.

**Command Mode**

Interface Configuration (Ethernet and port channel) and Interface Range (Ethernet and port channel)

**User Guidelines**

MMRP is not compatible with GVRP/GMRP. Do not enable MMRP on switches enabled for GVRP/GMRP.

Enabling MMRP on an interface automatically disables dynamic MFDB entry creation. MFDB entries are only configured via MMRP when MMRP is enabled.
Enabling MMRP on a port channel associated Ethernet interface has no effect as long as the interface is a member of the port channel. MMRP must also be enabled globally in order to become operational. This command is only available on the Dell EMC Networking N4000 Series switches.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example enables MMRP on port channel 1.
```
console(config)#interface po1
console(config-if-Po1)#mmrp
```

**mmrp global**
Use the `mmrp global` command to globally enable MMRP. Use the `no` form of the command to globally disable MMRP.

**Syntax**
```
mmrp global
no mmrp global
```

**Default Configuration**
By default, MMRP is disabled globally and on all interfaces.

**Command Mode**
Global Configuration

**User Guidelines**
MMRP is not compatible with GVRP/GMRP. Do not enable MMRP on switches enabled for GVRP/GMRP. IGMP snooping can interfere with MMRP/MVRP. Disable IGMP snooping if using MMRP/MVRP.
IGMP snooping can interfere with MMRP/MVRP. Disable IGMP snooping if using MMRP/MVRP.

MMRP propagates VLAN registration information to allow switches in the network to dynamically learn and configure VLANs. Refer to IEEE Std. 802.1Q-2005 and IEEE Std. 802.1Qbe-2010 for further information. In particular, MMRP must also be enabled on the individual interfaces to become operational.

MMRP does not support configuration of default group filtering behavior. MMRP does not support the optional Registrar Administrative Control for MAC addresses.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example enables MMRP globally.

```
console(config)#mmrp global
```

`mmrp periodic state machine`

Use this command to globally enable the MMRP periodic state machine. Use the no form of the command to globally disable the MMRP periodic state machine.

**Syntax**

```
mmrp periodic state machine
no mmrp periodic state machine
```

**Default Configuration**

By default, the MMRP periodic state machine is disabled globally.

**Command Mode**

Global Configuration
**User Guidelines**

The MMRP periodic state machine ages out unused MMRP entries. Use the `show mmrp summary` command to display the global MMRP administrative status.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example enables the MMRP periodic state machine.

```console
console(config)#mmrp periodic state machine
```

**show mmrp**

Use this command to display the MMRP configuration for an interface or globally.

**Syntax**

```
show mmrp [ summary | interface [ interface-id | summary ] ]
```

- `summary`—Show the global MMRP configuration.
- `interface-id`—Show the MMRP configuration for the specified interface.
- `interface summary`—Show the per interface MMRP configuration for all interfaces.

**Default Configuration**

This command has no defaults.

**Command Mode**

Privileged Exec, Global Configuration, and all submodes

**User Guidelines**

MMRP is not compatible the GMRP. Do not enable GMRP/GVRP on MMRP enabled switches.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console#show mmrp summary

MMRP Global Admin Mode........................ Disabled
MMRP Periodic State Machine.................... Disabled

console#show mmrp interface Gi1/0/12

MMRP Interface Admin Mode...................... Disabled

console#show mmrp interface summary

<table>
<thead>
<tr>
<th>Intf</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Disabled</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Disabled</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```

**show mmrp statistics**

Use this command to display the MMRP statistics for an interface or globally.

**Syntax**

```
show mmrp statistics {interface-id}
```

- interface-id—Displays the MMRP statistics for the specified interface.

**Default Configuration**

By default, the global statistics are displayed.

**Command Mode**

Privileged Exec, Global Configuration, and all submodes

**User Guidelines**

MMRP is not compatible with GMRP. Do not enable GMRP on MMRP enabled switches.
Command History

Introduced in version 6.2.0.1 firmware.

Example

console#show mmrp statistics gi1/0/12

Port........................................... Gi1/0/12
MMRP messages received......................... 21
MMRP messages received with bad header........ 0
MMRP messages received with bad format......... 0
MMRP messages transmitted...................... 8
MMRP messages failed to transmit............... 0
Multiple VLAN Registration Protocol Commands

Dell EMC Networking N4000 Series Switches

This section covers commands related to Multiple VLAN Registration Protocol (MVRP). MVRP is an implementation of IEEE 802.1ak in support of Audio-Video Bridging. Dell EMC Networking MVRP supports registration (dynamic VLAN creation) and propagation of VLAN membership information.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear mvrp statistics</th>
<th>mvrp periodic state machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvrp</td>
<td>show mvrp</td>
</tr>
<tr>
<td>mvrp global</td>
<td>show mvrp statistics</td>
</tr>
</tbody>
</table>

**clear mvrp statistics**

This command clears the MVRP statistics for an interface or all interfaces.

**Syntax**

clear mvrp statistics [ interface-id | all ]

- All—Clear MVRP statistics for all interfaces
- interface-id—Clear statistics for the specified interface.

**Default Configuration**

This command has no defaults.

**Command Mode**

Privileged Exec
**User Guidelines**

MVRP is not compatible with GVRP. Do not enable GMRP/GVRP on MVRP enabled switches.

The `clear counters` command also clears all MVRP statistics for all interfaces in addition to clearing other counters.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example clears the MVRP counters on port channel 1

```
clear mmrp statistics po1
```

**mvrp**

This command enables MVRP on a specific interface. Use the `no` form of the command to disable MVRP on an interface.

**Syntax**

```
mvrp
no mvrp
```

**Default Configuration**

By default, MVRP is disabled globally and on all interfaces.

**Command Mode**

Interface Configuration (Ethernet and port channel) and Interface Range (Ethernet and port channel)

**User Guidelines**

MVRP is not compatible with GVRP/GMRP. Do not enable MVRP on switches enabled for GVRP/GMRP.

MVRP operates in dynamic mode only. It both propagates VLAN configuration and learns (and creates) VLANs learned from the link peer.
Enabling MVRP on a port channel associated interface has no effect as long as the interface is a member of the port channel.

MVRP is not compatible with private VLAN configured interfaces. Do not enable GVRP on private VLAN enabled interfaces.

MVRP must also be enabled globally in order to become operational.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example enables MVRP on port channel 1

```
console(config)#interface po1
console(config-if-Po1)#mvrp
```

**mvrp global**

Use the `mvrp global` command to globally enable MVRP. Use the `no` form of the command to globally disable MVRP.

**Syntax**

```
mvrp global
no mvrp global
```

**Default Configuration**

By default, MVRP is disabled globally and on all interfaces.

**Command Mode**

Global Configuration mode

**User Guidelines**

MVRP is not compatible with GVRP/GMRP. Do not enable MVRP on switches enabled for GVRP/GMRP.
MVRP propagates VLAN registration information to allow switches in the network to dynamically learn and configure VLANs. Refer to IEEE Std. 802.1Q-2005 and IEEE Std. 802.1Qbe-2010 for further information. In particular, MVRP must also be enabled on the individual interfaces to become operational.

MVRP does not support configuration of default group filtering behavior. MVRP does not support the optional Registrar Administrative Control for VLANs.

If a VLAN is statically configured on an interface and MVRP requests registration (dynamic creation) of the VLAN, it is deleted and added back as a tagged static VLAN. If subsequently deleted by the operator, the VLAN is dynamically created.

If a VLAN is configured as forbidden on an interface and MVRP requests registration (dynamic creation) of the same VLAN, MVRP does not configure the port association.

MVRP is only supported on trunk or general mode ports.

This command is only available on the N4000 Series switches.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example enables MVRP globally.

```
console(config)#mvrp global
```

**mvrp periodic state machine**

Use this command to globally enable the MVRP periodic state machine. Use the no form of the command to globally disable the MVRP periodic state machine.

**Syntax**

```
mvrp periodic state machine
no mvrp periodic state machine
```
**Default Configuration**
By default, the MVRP periodic state machine is disabled globally.

**Command Mode**
Global Configuration

**User Guidelines**
The periodic state machine ages out MVRP created dynamic VLANs. Use the `show mvrp summary` command to display the global MVRP administrative status.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example enables the MVRP periodic state machine.
```
console(config)#mvrp periodic state machine
```

**show mvrp**
Use this command to display the MVRP configuration for an interface or globally.

**Syntax**
```
show mvrp [ summary | interface [ interface-id | summary ] ]
```
- `summary`—Show the global MMRP configuration.
- `interface-id`—Show the MMRP configuration for the specified interface.
- `interface summary`—Show the per interface MMRP configuration for all interfaces.

**Default Configuration**
This command has no defaults.
**Command Mode**
Privileged Exec, Global Configuration, and all submodes

**User Guidelines**
MVRP is not compatible with GMRP. Do not enable GMRP/GVRP on MVRP enabled switches.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
The following shows example CLI display output for the command.

```
console#show mvrp summary

MVRP global state.............................. Disabled
MVRP Periodic State Machine state............. Disabled
VLANs created via MVRP......................... 20-45, 3001-3050

The following shows example CLI display output for the command.
(Switching) #show mvrp interface 0/12

MVRP interface state........................... Enabled
VLANs declared.................................. 20-45, 3001-3050
VLANs registered............................... none

```

**show mvrp statistics**
Use this command to display the MVRP statistics for an interface or globally.

**Syntax**
```
show mvrp statistics {interface-id}
```

- interface-id—Displays the MVRP statistics for the specified interface.

**Default Configuration**
By default, the global statistics are displayed.

**Command Mode**
Privileged Exec, Global Configuration, and all submodes
User Guidelines
MVRP is not compatible with GMRP/GVRP. Do not enable GVRP on MMRP enabled switches.

Command History
Introduced in version 6.2.0.1 firmware.

Example
The following shows example CLI display output for the command.

```
console#show mvrp statistics summary
MVRF messages received........................ 45
MVRF messages received with bad header........ 0
MVRF messages received with bad format........ 0
MVRF messages transmitted...................... 16
MVRF messages failed to transmit............... 0
MVRF Message Queue Failures.................... 0

The following shows example CLI display output for the command.
(Switching) #show mvrp statistics 0/12
Port........................................... 0/12
MVRF messages received........................ 21
MVRF messages received with bad header........ 0
MVRF messages received with bad format........ 0
MVRF messages transmitted...................... 8
MVRF messages failed to transmit............... 0
MVRF failed reservations...................... 0
```
Multiple Stream Reservation Protocol Commands

Dell EMC Networking N4000 Series Switches

This section covers commands related to Multiple Stream Reservation Protocol (MSRP). MSRP supports registration of stream membership and resource reservation in support of Audio-Visual Bridging as defined by IEEE 802.1Qat and IEEE 802.1Qav. These commands are only available on the Dell EMC Networking N4000 Series switches.

Commands in this Section

This section explains the following commands:

- clear msrp statistics
- msrp srclassqav
- msrp (Interface)
- msrp talker-pruning
- msrp boundary-propagate
- show msrp
- msrp delta-bw
- show msrp reservations
- msrp global
- show msrp statistics
- msrp max-fan-in-ports
- show msrp stream
- msrp srclass-pvid
- show msrp statistics

**clear msrp statistics**

Use this command to clear the MSRP statistics for an interface or all interfaces.

**Syntax**

```
clear msrp statistics [ interface-id | all ]
```

- **all**—Clear MSRP statistics for all interfaces
- **interface-id**—Clear statistics for the specified interface. Argument must be a Ethernet interface identifier.
**Default Configuration**
This command has no defaults.

**Command Mode**
Privileged Exec

**User Guidelines**
The `clear counters` command also clears all MSRP statistics for all interfaces in addition to clearing other counters.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example clears the MSRP counters on interface Gi1/0/4
```
console#clear msrp statistics gi1/0/4
```

**msrp (Interface)**
Use this command to enable MSRP on a specific interface. Use the `no` form of the command to disable MSRP on an interface.

**Syntax**
```
msrp
no msrp
```

**Default Configuration**
By default, MSRP is disabled globally and on all interfaces.

**Command Mode**
Interface Configuration and Interface Range modes

**User Guidelines**
Enabling MSRP on a port channel associated interface has no effect as long as the interface remains a member of the port channel.
MSRP must also be enabled globally in order to become operational. This command is only available on the N4000 Series switches.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example enables MSRP on interface Gi1/0/1

```
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#msrp
```

**msrp boundary-propagate**
Use this command to configure the IEEE 802.1Qav boundary propagation. Use the no form of the command set the class configuration to the default.

**Syntax**

```
msrp boundary-propagate
no msrp boundary-propagate
```

**Default Configuration**
Talkers on a boundary port are ignored by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
Use the boundary propagation configuration to administratively define the edge of the IEEE 802.1Qav domain. Disable boundary propagation to ignore talkers on boundary ports.

Boundary propagation can only be configured when MSRP is globally disabled.

**Command History**
Introduced in version 6.2.0.1 firmware.
**Example**

This example administratively enables MSRP talker propagation from outside the domain.

```bash
console(config)#no msrp global
console(config)#msrp boundary-propagate
console(config)#msrp global
console(config)#show msrp summary
```

**msrp delta-bw**

Use this command to configure the MSRP VLAN ID for the SR traffic class on the interface.

**Syntax**

```bash
msrp delta-bw [a | b] bandwidth
no msrp delta-bw [a | b]
```

| bandwidth—The maximum percentage of bandwidth which may be reserved for a traffic class on an interface. The range is 0–75.

**Default Configuration**

By default, up to 75% of the interface bandwidth may be reserved for class A traffic and 0% may be reserved for class B traffic.

**Command Mode**

Interface Configuration mode (Ethernet and port channel), Interface range mode (Ethernet and port channel)

**User Guidelines**

MSRP must also be enabled globally in order to become operational.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configure MSRP delta bandwidth for class A traffic on interface Gi1/0/3 to be 50%

```bash
console(config)#interface gi1/0/3
console(config-if-Gi1/0/3)#msrp
console(config-if-Gi1/0/3)#msrp delta-bw a 50
```

**msrp global**

Use this command to globally enable MSRP. Use the `no` form of the command to globally disable MSRP.

**Syntax**

```bash
msrp global
no msrp global
```

**Default Configuration**

By default, MSRP is disabled globally and on all interfaces.

**Command Mode**

Global Configuration mode

**User Guidelines**

MSRP is not compatible with GMRP/GVRP. Do not enable GMRP/GVRP on MMRP/MVRP/MSRP enabled switches.

MSRP must also be enabled on individual interfaces to become operational.

MSRP propagates stream reservation registration information to/from talkers and listeners and implements admission. Refer to IEEE Std. 802.1Qat-2010 and IEEE 802.1Q-2011 for further information.
MSRP is internally mapped onto multicast queues 2 and 3. Generally, unicast traffic does not use these queues except for destination lookup failures which are broadcast to all ports in the VLAN. Delay limits are not calculated to accommodate such traffic.

Likewise, static configuration can place traffic onto the multicast queues and interfere with AVB traffic. Delay limits cannot be guaranteed in such cases. This command is only available on the N4000 Series switches.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example enables MSRP globally.

```
console(config)#msrp global
```

### msrp max-fan-in-ports

Use this command to configure the fan-in value used in calculating available bandwidth. Use the `no` form of the command to return the fan in to the default.

**Syntax**

```
msrp max-fan-in-ports fan-in
no msrp max-fan-in-ports
```

- **fan-in**—The fan in value used in the calculation of available bandwidth. The range is 0–52.

**Default Configuration**

The default fan-in value is 12.

**Command Mode**

Global Configuration
User Guidelines

This command configures the maximum number of ingress ports that are capable of transmitting into a single egress port (i.e., the maximum number of talker registrations on a switch). If the fan in is reduced below the number of active registrations, the switch attempts to remove the lowest priority registrations until the fan in limit is reached.

Command History

Introduced in version 6.2.0.1 firmware.

Example

This example configures the fan in to 14 interfaces.

```
console(config)#msrp max-fan-in-ports 14
console(config)#show msrp summary
```

```
MSRP Global Admin Mode......................... Enabled
MSRP Talker Pruning............................ Enabled
MSRP Maximum Fan-in Ports...................... 14
MSRP Boundary Propagation...................... Enabled
QAV class A priority............................ 4
QAV class A remap priority...................... 1
QAV class B priority............................ 3
QAV class B remap priority...................... 1
```

msrp srclass-pvid

Use this command to configure the MSRP VLAN ID for the SR traffic class on the interface.

Syntax

```
msrp srclass-pvid vlan-id
no msrp srclass-pvid
```

- `vlan-id`—The VLAN ID of the MSRP SR traffic. The range is 1–4093.

Default Configuration

By default, VLAN 2 is used to carry SR traffic.
**Command Mode**

Interface Configuration, Interface range

**User Guidelines**

The VLAN must be configured on the interface in order to carry traffic. The interface must be configured to carry tagged traffic (i.e., trunk mode). MSRP must also be enabled globally in order to become operational.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configure MSRP traffic on interface Gi1/0/2 for VLAN 12

```
console(config)#interface gi1/0/2
console(config-if-Gi1/0/2)#msrp
console(config-if-Gi1/0/2)#msrp srclass-pvid 12
```

**msrp srclassqav**

Use this command to configure the IEEE Qav class priority map. Use the no form of the command to set the class configuration to the default.

**Syntax**

```
msrp srclassqav class [a | b] [pcp | remap] 0-7
no msrp srclassqav class [ a | b ]
```

- **class a | b**—Specifies the class to be configured. Dell EMC Networking switches support class A and class B priorities.
- **pcp**—Specifies the priority of the selected MSRP traffic class. The range is 0–7. This is the value received in the Ethernet frame for trusted ports or assigned by the system as a default.
- **remap**—Specifies the priority of the non-AVB traffic with AVB traffic class PCP. The range is 0–7. This is the priority to which traffic is remapped.

**Default Configuration**

The defaults for the traffic classes are:
- Class A: pcp = 3, remap = 1
- Class B: pcp = 2, remap = 1

**Command Mode**

Global Configuration

**User Guidelines**

The IEEE802.1 Qav standard supports time-sensitive traffic streams by pacing all switch traffic, including legacy asynchronous Ethernet traffic, through queuing and forwarding. Dell EMC Networking switches support two stream reservation (SR) classes (A and B). Received traffic using a code point identified as belonging to class A or B are placed on a queue that uses a credit based shaper on egress. IEEE 802.1Qav does not specify any form of ingress metering or policing.

When an IEEE 802.1Qav talker registers a stream, it identifies whether the stream is class A or B and specifies the bandwidth required. Class A traffic has a higher transmission priority than class B traffic. The bandwidth that may be reserved is limited to 75% of the total bandwidth.

The priorities received in a frame are mapped onto traffic classes for trusted ports. See the output of the `show classofservice dot1pmapping` command for the mappings.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example maps class A traffic onto user priority 4.

```
console(config)#msrp srclassqav class a pcp 4
console(config)#show msrp summary
```

MSRP Global Admin Mode......................... Enabled
MSRP Talker Pruning.............................. Disabled
MSRP Maximum Fan-in Ports....................... 12
MSRP Boundary Propagation....................... Disabled
QAV class A priority............................ 4
QAV class A remap priority...................... 1
QAV class B priority............................ 2
QAV class B remap priority...................... 1
This example maps class B traffic onto user priority 3.

```
console(config)#msrp srcclassqav class b pcp 3
console(config)#show msrp summary

MSRP Global Admin Mode.......................... Enabled
MSRP Talker Pruning................................ Disabled
MSRP Maximum Fan-in Ports....................... 12
MSRP Boundary Propagation....................... Disabled
QAV class A priority................................ 4
QAV class A remap priority....................... 1
QAV class B priority............................... 3
QAV class B remap priority....................... 1
```

**msrp talker-pruning**

Use this command to enable source pruning. Use the `no` form of the command to disable source pruning.

**Syntax**

```
msrp talker-pruning
no msrp talker-pruning
```

**Default Configuration**

By default, talkers are not pruned.

**Command Mode**

Global Configuration

**User Guidelines**

Source pruning allows service users (such as a bridge) that are sources of frames destined for a number of groups, such as server stations or routers, to avoid unnecessary flooding of traffic on their local LANs in circumstances where there are no current group members in the network that wish to receive such traffic.

Talker pruning can only be configured if MSRP is globally disabled.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example administratively enables MSRP source pruning.

console(config)#no msrp global
console(config)#msrp talker-pruning
console(config)#msrp global
console(config)#show msrp summary

MSRP Global Admin Mode......................... Enabled
MSRP Talker Pruning............................ Enabled
MSRP Maximum Fan-in Ports...................... 12
MSRP Boundary Propagation...................... Enabled
QAV class A priority........................... 4
QAV class A remap priority..................... 1
QAV class B priority........................... 3
QAV class B remap priority..................... 1

**show msrp**

Use this command to display the MSRP configuration for an interface or globally.

**Syntax**

show msrp [ summary | interface [ interface-id | summary ] ]

- **summary**—Show global MSRP configuration information.
- **interface-id**—Show the MSRP configuration for the specified interface. The interface id must be a Ethernet interface identifier.
- **interface summary**—Show the per interface MSRP configuration for all interfaces

**Default Configuration**

This command has no defaults.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes.
User Guidelines

The following fields are displayed for the summary command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSRP Global Admin Mode</td>
<td>If MSRP global admin mode is enabled or disabled.</td>
</tr>
<tr>
<td>MSRP Talker Pruning</td>
<td>If MSRP talker pruning is enabled or disabled.</td>
</tr>
<tr>
<td>MSRP Maximum Fan-in Ports</td>
<td>The configured MSRP maximum fan-in ports value.</td>
</tr>
<tr>
<td>MSRP Boundary Propagation</td>
<td>If MSRP boundary propagation is enabled or disabled.</td>
</tr>
<tr>
<td>QAV class A priority</td>
<td>The class A priority for traffic class mapping.</td>
</tr>
<tr>
<td>QAV class A remap priority</td>
<td>The class A remap priority for traffic class mapping.</td>
</tr>
<tr>
<td>QAV class B priority</td>
<td>The class B priority for traffic class mapping.</td>
</tr>
<tr>
<td>QAV class B remap priority</td>
<td>The class B remap priority for traffic class mapping.</td>
</tr>
</tbody>
</table>

The following fields are displayed for the interface command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSRP Interface Admin Mode</td>
<td>If MSRP admin mode is enabled or disabled on the interface.</td>
</tr>
<tr>
<td>SRclass PVID</td>
<td>The MSRP VLAN ID configured for the SR traffic class on the interface.</td>
</tr>
<tr>
<td>MSRP class A Boundary port status</td>
<td>The status of the MSRP class A boundary port.</td>
</tr>
<tr>
<td>MSRP class B Boundary port status</td>
<td>The status of the MSRP class B boundary port.</td>
</tr>
<tr>
<td>MSRP QAV class A delta bandwidth</td>
<td>The MSRP delta bandwidth for SR traffic class A.</td>
</tr>
<tr>
<td>MSRP QAV class B delta bandwidth</td>
<td>The MSRP delta bandwidth for SR traffic class B.</td>
</tr>
<tr>
<td>MSRP QAV class A bandwidth (allocated/total)</td>
<td>The allocated and total bandwidth allocated to MSRP QAV class A.</td>
</tr>
</tbody>
</table>
The following fields are displayed for the interface summary command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>The interface for which information is displayed.</td>
</tr>
<tr>
<td>Mode</td>
<td>The current mode of the interface (enabled/disabled).</td>
</tr>
<tr>
<td>SrPVID</td>
<td>The MSRP VLAN ID for the SR traffic class on the interface.</td>
</tr>
<tr>
<td>A-Prio</td>
<td>The class A priority for the interface.</td>
</tr>
<tr>
<td>A-Remap</td>
<td>The remap class A priority for the interface.</td>
</tr>
<tr>
<td>B-Prio</td>
<td>The class B priority for the interface.</td>
</tr>
<tr>
<td>B-Remap</td>
<td>The remap class B priority for the interface.</td>
</tr>
<tr>
<td>Boundary (A/B)</td>
<td>If boundary propagation is enabled for class A and class B.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console#show msrp summary

MSRP Global Admin Mode......................... Enabled
MSRP Talker Pruning............................ Disabled
MSRP Maximum Fan-in Ports...................... 12
MSRP Boundary Propagation...................... Disabled
QAV class A priority........................... 3
QAV class A remap priority..................... 1
QAV class B priority........................... 2
```

Audio Visual Bridging Commands | 1144
QAV class B remap priority ..................... 1

console#show msrp interface Gi1/0/12

MSRP Interface Admin Mode...................... Enabled
SRclassPVID.................................... 2
MSRP class A Boundary port status.............. True
MSRP class B Boundary port status.............. True
MSRP QAV class A delta bandwidth............. 75
MSRP QAV class A delta bandwidth............. 0
MSRP class A bandwidth (allocated/total)...... 0 / 0
MSRP class B bandwidth (allocated/total)...... 0 / 0
MSRP total bandwidth (allocated/total)........ 0 / 0
QAV class A priority........................... 3
QAV class A remap priority..................... 1
QAV class B priority........................... 2
QAV class B remap priority..................... 1

console#show msrp interface summary

<table>
<thead>
<tr>
<th>Intf</th>
<th>Mode</th>
<th>SrPVID</th>
<th>A-Prio</th>
<th>A-Remap</th>
<th>B-Prio</th>
<th>B-Remap</th>
<th>Boundary(A/B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Enabled</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>True / True</td>
</tr>
</tbody>
</table>

**show msrp reservations**

Use this command to display the MSRP reservation information for an interface.

**Syntax**

```
show msrp reservations [interface-id] [detail | summary]
```

- **interface-id**—An interface identifier (Ethernet).
- **detail**—Show detailed information on the reservations.
- **summary**—Show summary information on the reservations.

**Default Configuration**

This command has no defaults.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**
Use the `clear msrp statistics` command to clear the MMRP counters.
The `clear counters` command also clears all MSRP statistics for all interfaces in addition to clearing other counters.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console#show msrp reservations gi1/0/10 summary
Stream   Stream             Talker  Listener  Fail Information  Stream
ID       MAC Address        Type    Type      Code  Interface   Age
------   ----------------  ------  --------   ---------------  -----  
```
```
console#show msrp reservations gi1/0/10 detail
Stream   Stream             Failure Information          Acc
ID       MAC Address        Code Intf MAC Address    Latency
-------  -----------------  ---------------------------  ---------
41543    12:22:e1:65:a3:f8  0    0    00:00:00:00:00:00  647
```

**show msrp statistics**
Use this command to display the MSRP statistics for an interface or globally.

**Syntax**
```
show msrp statistics { interface-id }
```
- interface-id—Show the MSRP statistics for the specified interface.

**Default Configuration**
By default, the global statistics are shown.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**
The following information is displayed for the summary command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSRP messages received</td>
<td>The number of MSRP messages that have been received.</td>
</tr>
<tr>
<td>MSRP messages received with bad header</td>
<td>The number of MSRP messages that have been received with a bad header.</td>
</tr>
<tr>
<td>MSRP messages received with bad format</td>
<td>The number of MSRP messages that have been received in a bad format.</td>
</tr>
<tr>
<td>MSRP messages transmitted</td>
<td>The number of MSRP messages that have been transmitted.</td>
</tr>
<tr>
<td>MSRP messages failed to transmit</td>
<td>The number of MSRP messages that failed to transmit.</td>
</tr>
<tr>
<td>MSRP messages Queue Failures</td>
<td>The number of MSRP message queue failures.</td>
</tr>
</tbody>
</table>

The following information is displayed for the statistics command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface port number.</td>
</tr>
<tr>
<td>MSRP messages received</td>
<td>The number of MSRP messages that have been received.</td>
</tr>
<tr>
<td>MSRP messages received with bad header</td>
<td>The number of MSRP messages that have been received with a bad header.</td>
</tr>
<tr>
<td>MSRP messages received with bad format</td>
<td>The number of MSRP messages that have been received in a bad format.</td>
</tr>
<tr>
<td>MSRP messages transmitted</td>
<td>The number of MSRP messages that have been transmitted.</td>
</tr>
<tr>
<td>MSRP messages failed to transmit</td>
<td>The number of MSRP messages that failed to transmit.</td>
</tr>
</tbody>
</table>
Audio Visual Bridging Commands

MSRP failed registrations | The number of MSRP failed registrations.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console# show msrp statistics summary
MSRP messages received............................ 1790
MSRP messages received with bad header......... 0
MSRP messages received with bad format........ 0
MSRP messages transmitted....................... 830
MSRP messages failed to transmit............... 0
MSRP Message Queue Failures..................... 0

console# show msrp statistics gi1/0/10
Port.................................................. Gi1/0/10
MSRP messages received............................ 741
MSRP messages received with bad header......... 0
MSRP messages received with bad format......... 0
MSRP messages transmitted....................... 674
MSRP messages failed to transmit............... 0
MSRP failed registrations......................... 0

show msrp stream
Use this command to display MSRP stream information.

Syntax
show msrp stream [ detail | summary ]
  • detail—Show detailed information on the streams.
  • summary—Show summary information on the streams.

Default Configuration
The command has no defaults.

Command Mode
Privileged Exec mode, Global Configuration mode and all sub-modes.
User Guidelines

The following information is displayed for the detail command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Talker ID</td>
<td>The MSRP stream talker ID.</td>
</tr>
<tr>
<td>Stream MAC Address</td>
<td>The MSRP stream MAC address.</td>
</tr>
<tr>
<td>Traff Class</td>
<td>The MSRP traffic class.</td>
</tr>
<tr>
<td>Stream TSpec</td>
<td>The MSRP stream TSpec.</td>
</tr>
<tr>
<td>Failure Code</td>
<td>The MSRP failure code.</td>
</tr>
<tr>
<td>Failure Intf</td>
<td>The MSRP interface.</td>
</tr>
<tr>
<td>Failure MAC Address</td>
<td>The MSRP MAC address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port interface.</td>
</tr>
</tbody>
</table>

The following information is displayed for the summary command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Talker ID</td>
<td>The MSRP stream talker ID.</td>
</tr>
<tr>
<td>Stream MAC Address</td>
<td>The MSRP stream MAC address.</td>
</tr>
<tr>
<td>Destination MAC Address</td>
<td>The destination MAC address.</td>
</tr>
<tr>
<td>Acc. Latency</td>
<td>The MSRP stream latency.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>Stream Rank</td>
<td>The MSRP stream rank.</td>
</tr>
</tbody>
</table>

Command History

Introduced in version 6.2.0.1 firmware.

Example

console#show msrp stream detail

<table>
<thead>
<tr>
<th>Stream ID</th>
<th>Stream MAC Address</th>
<th>Traff Class</th>
<th>Stream TSpec</th>
<th>Failure Code</th>
<th>Failure Intf</th>
<th>Failure MAC Address</th>
<th>Talker Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>41543</td>
<td>12:22:e1:65:a3:f8</td>
<td>A</td>
<td>128 1</td>
<td>0</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>Gi1/0/10</td>
</tr>
</tbody>
</table>
console#show msrp stream summary

<table>
<thead>
<tr>
<th>Stream ID</th>
<th>MAC Address</th>
<th>Destination MAC Address</th>
<th>Latency</th>
<th>VLAN ID</th>
<th>Stream Rank</th>
<th>Stream Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>41543</td>
<td>12:22:e1:65:a3:f8</td>
<td>01:00:00:80:42:01</td>
<td>647</td>
<td>2</td>
<td>Regular</td>
<td></td>
</tr>
</tbody>
</table>
802.1AS Timesync Commands

Dell EMC Networking N4000 Series Switches

This section covers commands related to IEEE 802.1AS timesync. The Dell EMC Networking 802.1AS capability implements the 2008 PTP Version 2 of the IEEE 1588 protocol in support of Audio-Visual Bridging. Dell EMC Networking 802.1AS implements the best master clock algorithm to select a precise time source and to measure propagation delay accurately. Dell EMC Networking switches are not Grand Master clock capable. A Grand Master clock time source must be supplied for a precise measurement of propagation delay.

Commands in this Section

This section explains the following commands:

- clear dot1as statistics
- dot1as (Global Configuration)
- dot1as (Interface Configuration)
- dot1as priority
- dot1as interval announce
- dot1as interval sync
- dot1as interval pdelay

<table>
<thead>
<tr>
<th>clear dot1as statistics</th>
<th>dot1as timeout announce</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1as (Global Configuration)</td>
<td>dot1as timeout sync</td>
</tr>
<tr>
<td>dot1as (Interface Configuration)</td>
<td>dot1as pdelay-threshold</td>
</tr>
<tr>
<td>dot1as priority</td>
<td>dot1as interval pdelay-loss</td>
</tr>
<tr>
<td>dot1as interval announce</td>
<td>show dot1as</td>
</tr>
<tr>
<td>dot1as interval sync</td>
<td>show dot1as statistics</td>
</tr>
<tr>
<td>dot1as interval pdelay</td>
<td>--</td>
</tr>
</tbody>
</table>

**clear dot1as statistics**

Use this command to clear the IEEE 802.1AS statistics for an interface or all interfaces.

**Syntax**

clear dot1as statistics [ interface-id ]

- All—Clear 802.1AS statistics for all interfaces.
- interface-id—Clear 802.1AS statistics for the specified interface.
Default Configuration
This command has no defaults.

Command Mode
Privileged Exec.

User Guidelines
The clear counters command also clears all IEEE 802.1AS statistics for all interfaces in addition to clearing other counters.

Command History
Introduced in version 6.2.0.1 firmware.

Example
This example clears the 802.1AS counters on port channel 1

```
console#clear dot1as statistics po1
```

**dot1as (Global Configuration)**
Use this command to globally enable IEEE 802.1AS. Use the `no` form of the command to globally disable IEEE 802.1AS.

**Syntax**

dot1as

no dot1as

**Default Configuration**
By default, IEEE 802.1AS is disabled globally and on all interfaces.

**Command Mode**
Global Configuration
**User Guidelines**

IEEE 802.1AS propagates time information from master clocks and synchronizes internally with the clock in support of delivering streams to the destination device with the same relative timing as sampled at the source.

All IEEE 802.1AS interfaces must reside on the same stack member. Propagation of timing information across a stack is not supported.

IEEE 802.1AS must also be enabled on individual interfaces to become operational.

This command is only available on the N4000 Series switches.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config)#dot1as
```

**dot1as (Interface Configuration)**

Use this command to enable IEEE 802.1AS on an interface. Use the `no` form of the command to disable IEEE 802.1AS on an interface.

**Syntax**

```
dot1as
no dot1as
```

**Default Configuration**

By default, IEEE 802.1AS is disabled globally and on all interfaces.

**Command Mode**

Interface Configuration

**User Guidelines**

IEEE 802.1AS propagates time information from master clocks and synchronizes with the internal clock in support of delivering streams to the destination device with the same relative timing as sampled at the source.
All IEEE 802.1AS interfaces must reside on the same stack member. Propagation of timing information across a stack is not supported.
IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#dot1as
```

**dot1as priority**
Use this command to globally configure the priority 1 or priority 2 value. Use the `no` form of the command to return the priority value to the default.

**Syntax**
```
dot1as priority [ 1 | 2 ] [ priority-value]
no dot1as priority [ 1 | 2 ]
```
- **priority [ 1 | 2 ]** — Selects the priority value to configure. Priority 1 and 2 are used in the selection of the grand master clock.

**Default Configuration**
By default, priority 1 is 246 and priority 2 is 248.

**Command Mode**
Global Configuration

**User Guidelines**
The best master clock algorithm considers the priority1 attribute before any other attributes; therefore, the priority1 attribute can be used to force a desired ordering of time-aware end stations with respect to best master clock selection.
IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.
IEEE 802.1AS propagates time information from master clocks and synchronizes internally with the clock in support of delivering streams to the destination device with the same relative timing as sampled at the source. While disabled, IEEE 802.1AS configuration is retained and can be changed, but is not operationally active.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures a switch as grand master capable.

```
console(config)#dot1as priority 1 255
console(config)#show dot1as summary

802.1AS Global Admin Mode.......................... Enabled
Grandmaster Capable.................................. Yes
Best Clock Identity..................................... 00:1E:C9:FF:FE:DE:B1:37
Best Clock Priority1.................................. 255
Best Clock Priority2.................................. 248
Steps to Best Clock.................................... 0
Local Clock Identity.................................... 00:1E:C9:FF:FE:DE:B1:37
Local Clock Priority1.................................. 255
Local Clock Priority2.................................. 248
Grandmaster Change Count............................ 0
Last Grandmaster Change Timestamp................... 0
```

**dot1as interval announce**

Use this command to configure the initial log announcement interval for an interface. Use the no form of the command to return the announcement interval to the default.

**Syntax**

dot1as interval announce int-val

no dot1as interval announce

- int-val—The initial log announcement interval in log base 2 format. The range is –5 to 5.
**Default Configuration**

By default, the announcement interval is 0.

**Command Mode**

Interface Configuration

**User Guidelines**

The initial log announcement interval is used to initialize the value of announce interval; it is the mean time interval between transmission of successive ANNOUNCE messages. The ANNOUNCE interval may be modified by the operation of the protocol (i.e., it is set to the initial value when the port is initialized and when a signaling message is received with a field announce interval set to 126). It may also be modified if the port receives a signaling message that carries a message interval request TLV.

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

IEEE 802.1AS propagates time information from master clocks and synchronizes internally with the clock in support of delivering streams to the destination device with the same relative timing as sampled at the source.

While disabled, IEEE 802.1AS configuration is retained and can be changed, but is not operationally active.

Refer to IEEE Std. 802.1AS-2011 and IEEE Std. 1588-2008 for further information on the initialLogAnnounceInterval attribute.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures the switch with an initial log announcement interval of 3.

```
console(config-if-Gi1/0/1)#dot1as interval announce 3
console(config-if-Gi1/0/1)#show dot1as interface gi1/0/1
```

802.1AS Interface Admin Mode.................. Enabled
802.1AS Capable................................ No
Is Measuring Delay......................... No
Propagation Delay.............................. 0
Port Role...................................... Disabled
PDELAY Threshold............................... 2500
PDELAY lost responses allowed.............. 3
Neighbor Rate Ratio............................ 0
Initial Sync Interval.......................... -3
Current Sync Interval.......................... -3
Initial Pdelay Interval........................ 0
Current Pdelay Interval........................ 0
Initial Announce Interval...................... 3
Current Announce Interval...................... 0
Sync Receipt Timeout........................... 3
Announce Receipt Timeout....................... 3

dot1as interval sync

Use this command to configure the sync interval for an interface. Use the no form of the command to return the sync interval to the default.

Syntax

dot1as interval sync int-val
no dot1as interval sync

- int-val—The time sync interval in log base 2 format. The range is –5 to 5.

Default Configuration

By default, the initial sync interval is –3.

Command Mode

Interface Configuration

User Guidelines

This value is the logarithm to the base 2 of the desired mean time interval between successive time-synchronization event messages sent by the link peer.

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures the switch with an initial log sync interval of 3.

```
console(config-if-Gi1/0/1)#dot1as interval sync 3
console(config-if-Gi1/0/1)#show dot1as interface gi1/0/1
```

```
AS Interface Admin Mode................... Enabled
AS Capable.................................. No
Is Measuring Delay.......................... No
Propagation Delay.......................... 0
Port Role.................................... Disabled
PDELAY Threshold........................... 2500
PDELAY lost responses allowed............ 3
Neighbor Rate Ratio.......................... 0
Initial Sync Interval......................... 3
Current Sync Interval....................... -3
Initial Pdelay Interval....................... 0
Current Pdelay Interval...................... 0
Initial Announce Interval.................... 3
Current Announce Interval................... 0
Sync Receipt Timeout......................... 3
Announce Receipt Timeout.................... 3
```

dot1as interval pdelay

Use this command to configure the pdelay interval for an interface. Use the no form of the command to return the pdelay interval to the default.

**Syntax**

dot1as interval pdelay int-val

no dot1as interval pdelay

- int-val—The initial pdelay interval in log base 2 format. The range is –5 to 5.

**Default Configuration**

By default, the pdelay interval is 0.
**Command Mode**

Interface Configuration

**User Guidelines**

This value is the logarithm to the base 2 of the desired mean time interval between successive Pdelay_req messages sent by the link peer. IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures the switch with an initial log sync interval of 3.

```
console(config-if-Gi1/0/1)#dot1as interval pdelay 3
console(config-if-Gi1/0/1)#show dot1as interface gi1/0/1
```

<table>
<thead>
<tr>
<th>AS Interface Admin Mode</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Capable</td>
<td>No</td>
</tr>
<tr>
<td>Is Measuring Delay</td>
<td>No</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>0</td>
</tr>
<tr>
<td>Port Role</td>
<td>Disabled</td>
</tr>
<tr>
<td>PDELAY Threshold</td>
<td>2500</td>
</tr>
<tr>
<td>PDELAY lost responses allowed</td>
<td>3</td>
</tr>
<tr>
<td>Neighbor Rate Ratio</td>
<td>0</td>
</tr>
<tr>
<td>Initial Sync Interval</td>
<td>3</td>
</tr>
<tr>
<td>Current Sync Interval</td>
<td>-3</td>
</tr>
<tr>
<td>Initial Pdelay Interval</td>
<td>3</td>
</tr>
<tr>
<td>Current Pdelay Interval</td>
<td>0</td>
</tr>
<tr>
<td>Initial Announce Interval</td>
<td>3</td>
</tr>
<tr>
<td>Current Announce Interval</td>
<td>0</td>
</tr>
<tr>
<td>Sync Receipt Timeout</td>
<td>3</td>
</tr>
<tr>
<td>Announce Receipt Timeout</td>
<td>3</td>
</tr>
</tbody>
</table>

**dot1as timeout announce**

Use this command to configure the number of announce intervals expiries with no received announce message in which case the master is considered to be no longer transmitting. Use the no form of the command to return the announce expiries to the default.
Syntax

dot1as timeout announce expiries

no dot1as timeout announce

• expiries—The number of expiries with no received announce message on which the master is considered to be no longer transmitting. The range is 2–255.

Default Configuration

By default, the number of expiries is set to 3.

Command Mode

Interface Configuration

User Guidelines

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

Command History

Introduced in version 6.2.0.1 firmware.

Example

This example configures interface Gi1/0/4 to delay expiring the master clock, if found, for up to 5 announce intervals.

    console(config-if-Gi1/0/4)#dot1as timeout announce 5
    console(config-if-Gi1/0/4)#show dot1as interface gi1/0/4

    AS Interface Admin Mode................... Enabled
    AS Capable........................................ No
    Is Measuring Delay.............................. No
    Propagation Delay........................... 0
    Port Role........................................ Disabled
    PDELAY Threshold......................... 2500
    PDELAY lost responses allowed............... 3
    Neighbor Rate Ratio......................... 0
    Initial Sync Interval........................ -3
    Current Sync Interval....................... -3
    Initial Pdelay Interval...................... 3
    Current Pdelay Interval..................... 0
**Initial Announce Interval**.......................... 0
**Current Announce Interval**.......................... 0
**Sync Receipt Timeout**........................... 3
**Announce Receipt Timeout**....................... 5

**dot1as timeout sync**

Use this command to configure the number of sync intervals expiries with no received announce message in which case the master is considered to be no longer transmitting. Use the no form of the command to return the sync-expiries to the default.

**Syntax**

dot1as timeout sync expiries
no dot1as timeout announce

**Default Configuration**

By default, the number of expiries is set to 3.

**Command Mode**

Interface Configuration

**User Guidelines**

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures interface Gi1/0/4 to delay expiring the master clock, if found, for up to 5 sync intervals.

console(config-if-Gi1/0/4)#dot1as timeout sync 5
console(config-if-Gi1/0/4)#show dot1as interface gi1/0/4

AS Interface Admin Mode....................... Enabled
AS Capable........................................ No
dot1as pdelay-threshold

Use this command to configure the propagation delay threshold in nanoseconds, above which an interface is not considered capable of participating in the AS protocol.

Use the no form of the command to return the threshold to the default.

**Syntax**

dot1as pdelay-threshold thresh-val

no dot1as pdelay-threshold

**Default Configuration**

By default, the number of expiries is set to 2500 nanoseconds for copper interfaces and 8000 nanoseconds for fiber thresholds.

**Command Mode**

Interface Configuration

**User Guidelines**

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.
Command History
Introduced in version 6.2.0.1 firmware.

Example
This example configures interface Gi1/0/4 to delay retiring the interface for 10 ms.

```bash
console(config-if-Gi1/0/4)#dot1as pdelay-threshold 10000
console(config-if-Gi1/0/4)#show dot1as interface gi1/0/4
```

AS Interface Admin Mode................... Enabled
AS Capable................................. No
Is Measuring Delay........................ No
Propagation Delay............................ 0
Port Role..................................... Disabled
PDELAY Threshold........................... 10000
PDELAY lost responses allowed............. 3
Neighbor Rate Ratio........................... 0
Initial Sync Interval....................... -3
Current Sync Interval....................... -3
Initial Pdelay Interval..................... 3
Current Pdelay Interval..................... 0
Initial Announce Interval................... 3
Current Announce Interval................... 0
Sync Receipt Timeout....................... 5
Announce Receipt Timeout................... 3

dot1as interval pdelay-loss

Use this command to configure the number of Pdelay_Req messages for which a valid response has not been received, above which a port is considered to not be exchanging peer delay messages with its neighbor. Use the no form of the command to return the interval to the default.

Syntax
dot1as interval pdelay-loss expiries
no dot1as interval pdelay-loss

- expiries—The number of expiries with no received Pdelay_Resp message after which the port is no longer considered to be exchanging messages with the peer. The range is 0–65535.
**Default Configuration**

By default, the number of expiries is set to three responses. If three Pdelay Resp messages are received within that time, the port is considered to be no longer exchanging messages with the peer.

**Command Mode**

Interface Configuration

**User Guidelines**

IEEE 802.1AS must also be enabled globally as well as on an interface to become operational.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example configures interface Gi1/0/4 to delay retiring the interface for 10 ms.

```
console(config-if-Gi1/0/4)#dot1as interval pdelay-loss 5
console(config-if-Gi1/0/4)#show dot1as interface gi1/0/4
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Interface Admin Mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>AS Capable</td>
<td>No</td>
</tr>
<tr>
<td>Is Measuring Delay</td>
<td>No</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>0</td>
</tr>
<tr>
<td>Port Role</td>
<td>Disabled</td>
</tr>
<tr>
<td>PDELAY Threshold</td>
<td>10000</td>
</tr>
<tr>
<td>PDELAY lost responses allowed</td>
<td>5</td>
</tr>
<tr>
<td>Neighbor Rate Ratio</td>
<td>0</td>
</tr>
<tr>
<td>Initial Sync Interval</td>
<td>-3</td>
</tr>
<tr>
<td>Current Sync Interval</td>
<td>-3</td>
</tr>
<tr>
<td>Initial Pdelay Interval</td>
<td>3</td>
</tr>
<tr>
<td>Current Pdelay Interval</td>
<td>0</td>
</tr>
<tr>
<td>Initial Announce Interval</td>
<td>3</td>
</tr>
<tr>
<td>Current Announce Interval</td>
<td>0</td>
</tr>
<tr>
<td>Sync Receipt Timeout</td>
<td>5</td>
</tr>
<tr>
<td>Announce Receipt Timeout</td>
<td>3</td>
</tr>
</tbody>
</table>
show dot1as

Use this command to show the IEEE 802.1AS configuration for an interface or globally.

Syntax

show dot1as [ summary | interface [ interface-id | summary ] ]

- summary—Show the global IEEE 802.1AS configuration.
- interface-id—Show the IEEE 802.1AS configuration for the specified interface.
- interface summary—Show the per interface IEEE 802.1AS configuration for all interfaces.

Default Configuration

The command has no defaults.

Command Mode

Privileged Exec, Global Configuration, and all sub-modes

User Guidelines

The following information is displayed for the summary command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Global Admin Mode</td>
<td>Configured value of AS global admin mode.</td>
</tr>
<tr>
<td>Grandmaster Present</td>
<td>Indicates where a AS grandmaster is present or not.</td>
</tr>
<tr>
<td>Best Clock Identity</td>
<td>Specifies the clock identity of the AS grandmaster.</td>
</tr>
<tr>
<td>Best Clock Priority1</td>
<td>Specifies the priority1 value of AS grandmaster.</td>
</tr>
<tr>
<td>Best Clock Priority2</td>
<td>Specifies the priority2 value of AS grandmaster.</td>
</tr>
<tr>
<td>Steps to Best Clock</td>
<td>Specifies the number of hops between the local clock and the grandmaster.</td>
</tr>
<tr>
<td>Local Clock Identity</td>
<td>Specifies the clock identity of the local clock.</td>
</tr>
<tr>
<td>Local Clock Priority1</td>
<td>Specifies the priority1 value of AS local clock.</td>
</tr>
<tr>
<td>Local Clock Priority2</td>
<td>Specifies the priority2 value of local clock.</td>
</tr>
</tbody>
</table>
The following information is displayed for the interface command.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grandmaster Change Count</td>
<td>Specifies the number of GM change events occurred.</td>
</tr>
<tr>
<td>Last Grandmaster Change</td>
<td>Specifies the timestamp of the last GM change event.</td>
</tr>
<tr>
<td>Latch Time Stamp</td>
<td></td>
</tr>
<tr>
<td>Interface Description</td>
<td></td>
</tr>
</tbody>
</table>

**Field**

- **Intf**
  - Slot/port

- **Mode**
  - IEEE 802.1AS interface admin mode (enabled/disabled)

- **asCapable**
  - Indicates if the interface is asCapable.

- **measuringPdelay**
  - Indicates if the interface is measuring PDELAY.

- **Pdelay**
  - Indicates the value of the propagation delay on this interface.

- **Role**
  - Indicates one of the IEEE 802.1AS port roles (MASTER, SLAVE, PASSIVE, DISABLED)

- **Pdelay Threshold**
  - Specifies the propagation delay threshold in nanoseconds, above which an interface is not considered capable of participating in the AS protocol.

- **Pdelay lost responses allowed**
  - Specifies the number of Pdelay_Req messages for which a valid response is not received, above which a port is considered to not be exchanging peer delay messages with its neighbor.

- **Neighbor Rate Ratio**
  - Specifies an estimate of the ratio of the frequency of the LocalClock entity of the time-aware system at the other end of the link attached to this port, to the frequency of the LocalClock entity of this time-aware system.

- **Initial Pdelay interval**
  - Specifies the configured mean time interval between successive PDELAY_REQ messages sent over a link, in logarithm to base 2 format.

- **Initial Announce Interval**
  - Specifies the configured mean time interval between successive ANNOUNCE messages in logarithm to base 2 format.
Audio Visual Bridging Commands

## Command History

Introduced in version 6.2.0.1 firmware.

## Example

```
console#show dot1as interface summary

<table>
<thead>
<tr>
<th>Intf</th>
<th>Mode</th>
<th>asCapable</th>
<th>measuringPdelay</th>
<th>Pdelay</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Enabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Disabled</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>811</td>
<td>Master</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enabled</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>Disabled</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>806</td>
<td>Master</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Enabled</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```

```
console#show dot1as interface gi1/0/1

AS Interface Admin Mode.................. Enabled
AS Capable................................ No
Is Measuring Delay....................... No
Propagation Delay....................... 0
```
Port Role...................................... Disabled
PDELAY Threshold......................... 2500
PDELAY lost responses allowed........... 3
Neighbor Rate Ratio.......................... 0
Initial Sync Interval....................... -5
Initial Pdelay Interval..................... 3
Initial Announce Interval................. 5
Current Sync Interval...................... 0
Current Pdelay Interval.................... 0
Current Announce Interval............... 0
Sync Receipt Timeout...................... 3
Announce Receipt Timeout................ 3

console#show dot1as summary

AS Global Admin Mode......... Enabled
Grandmaster Present............. TRUE
Best Clock Identity.............. 02:10:18:FF:FE:57:80:10
Best Clock Priority1........... 127
Best Clock Priority2........... 255
Steps to Best Clock............... 1
Local Clock Identity............. 00:10:18:FF:FE:82:11:DB
Local Clock Priority1.......... 246
Local Clock Priority2.......... 248
Grandmaster Change Count......... 5
Last Grandmaster Change Timestamp.. 2819202563

show dot1as statistics
Use this command to show the IEEE 802.1AS statistics for an interface.

Syntax
show dot1as statistics [ interface-id ]

- interface-id—Show statistics for the specified interface.

Default Configuration
This command has no defaults.

Command Mode
Privileged Exec, Global Configuration, and all sub-modes
**User Guidelines**

Use the `clear dot1as statistics` or the `clear counters` command to clear the counters.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
#show dot1as statistics gi1/0/3

Port........................................... Gi1/0/3
Sync messages transmitted................ 0
Sync messages received.................... 0
Followup messages transmitted............ 0
Followup messages received................ 0
Announce messages transmitted............ 0
Announce messages received................ 0
Pdelay_Req messages transmitted.......... 0
Pdelay_Req messages received............. 0
Pdelay_Resp messages transmitted......... 0
Pdelay_Resp messages received............ 0
Pdelay_Resp_Followup messages transmitted. 0
Pdelay_Resp_Followup messages received.. 0
Signaling messages transmitted........... 0
Signaling messages received.............. 0
Sync receipt timeouts....................... 0
Sync messages discarded.................. 0
Announce receipt timeouts................ 0
Announces messages discarded............ 0
Pdelay receipt timeouts.................... 0
Pdelay messages discards.................. 0
PTP message discards..................... 0
Pdelay allowed lost responses............ 0
Invalid AS messages received............. 0
```
Data Center Technology Commands

Dell EMC Networking N4000 Series Switches

The data center commands allow network operators to deploy lossless Ethernet capabilities in support of a converged network with Fibre Channel and Ethernet data, as specified by the FC-BB-5 working group of ANSI T11. This capability allows operators to deploy networks at a lower cost while still maintaining the same SAN network management operations that exists today.

**NOTE:** Data Center Technologies such as ETS, DCBX, and PFC are only available on Dell EMC Networking N4000 series switches.

This section of the document contains the following data center bridging commands:

- Data Center Bridging Commands
- OpenFlow Commands
- Priority Flow Control Commands
Data Center Bridging Commands

Dell EMC Networking N4000 Series Switches

NOTE: Enhanced Transmission Selection commands are only supported on N4000 series switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.

Data Center Bridging Exchange Protocol

The Data Center Bridging Exchange Protocol (DCBX) is used by DCB devices to exchange configuration information with directly connected peers. The protocol is also used to detect misconfiguration of the peer DCB devices and, optionally, for configuration of peer DCB devices.

DCBX is expected to be deployed in support of lossless operation for FCoE or iSCSI traffic. In these scenarios, all network elements are DCBX-enabled (DCBX is enabled end-to-end).

The Dell EMC Networking implementation of the DCBX protocol supports the propagation of configuration information for the following features:

1. Enhanced Transmission Selection (ETS)
2. Priority-based Flow Control (PFC)
3. Application Priorities

The features listed above use DCBX to send and receive device configuration and capability information and configuration details to peer DCBX devices. The PFC and ETS information exchange is discussed in Priority Flow Control Commands and Enhanced Transmission Selection. Application Priority information is captured from the configuration source and propagated to other auto-configuration peers by the DCBX component. When iSCSI is enabled on an operationally active PFC port, the application priority information is supplemented with the configured iSCSI priority.

Enhanced Transmission Selection

NOTE: Enhanced Transmission Selection commands are only supported on N4000 series switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.
In a typical switch or router, each Ethernet port supports one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the device.

The drop precedence of a packet is an indication of whether the packet is more or less likely to be dropped during times of queue congestion. Often referred to as packet coloring, a low drop precedence (green) allows the packet to be transmitted under most circumstances, a higher drop precedence (yellow) subjects the packet to dropping when bursts become excessive, while the highest drop precedence (red) discards the packet whenever the queue is congested. In some hardware implementations, the queue depth can be managed using tail dropping or a weighted random early discard, or a weighted random early discard (WRED), technique. These methods often use customizable threshold parameters that are specified on a per-drop-precedence basis.

The Dell EMC Networking QoS implementation contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors. However, the DiffServ feature does not offer direct configuration of the hardware CoS queue resources.

The CoS Queuing feature offers a new capability for the user to directly configure certain aspects of device queuing to provide the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics such as minimum guaranteed bandwidth, transmission rate shaping, etc. are now user configurable at the queue (or port) level.

The CoS queue feature provides a method to configure Traffic Class Groups (TCGs) to extend the CoS queue management. Multiple CoS queues can be mapped to a single TCG. Each TCG can have a configured minimum guaranteed bandwidth allocation and a scheduling algorithm similar to the
CoS queue configuration. The TCG scheduling and bandwidth enforcement occurs after the CoS queue scheduling and bandwidth enforcement is performed. Therefore all CoS queues mapped to the same TCG share the scheduling and bandwidth properties of the TCG.

**ETS Operations**

ETS provides an operational model for priority processing and bandwidth allocation for the switch in a Data Center Bridging environment. Using priority-based processing and bandwidth allocations, different Traffic Class Groups (TCGs) within different types of traffic such as LAN, SAN and Management can be configured to provide bandwidth allocation or best effort transmit characteristics.

For ETS to be operational, the following configuration steps need to be performed:

1. Configure CoS queues to Traffic Class Group mapping for the egress ports.
2. Configure weight percentage (bandwidth allocation) for each TCG.
3. Enable appropriate scheduling algorithm for each TCG.

CoS information is exchanged with peer DCBX devices using ETS TLVs. As part of the transmitted ETS TLVs, by default, DCBX advertises the following parameters, and these parameters are populated in the switch hardware on a per port basis.

1. Mapping between ingress ports 802.1p priority to Traffic Class Group (TCG).
2. Bandwidth percentage (weight percentage) of each Traffic Class Group.
3. Scheduling algorithm for each Traffic Class Group.

For Dell EMC Networking switches which do not support configuration of ETS traffic classes in the hardware, the ETS information is propagated from the configuration source to the other DCBX peers.

The mapping between the ingress port’s 802.1p priority and TCG is not direct. The mapping depends upon:

- The CoS map defining the CoS queue that a packet is egress forwarded for the ingress 802.1p priority.
- Traffic Class Group map defining the CoS queue to TCG mapping.
The indirect mapping between the 802.1p priorities and the associated Traffic Class Group mapping is advertised by DCBX as part of ETS TLVs. For this indirect mapping to be valid, the following parameters need to be configured in addition to the configuration of the TCGs.

1. Configure 802.1p priority to CoS mapping for the ingress ports.
2. Enable Trust mode on the ingress ports to trust the 802.1p priority present in the frames.

ETS TLVs use DCBX Asymmetric attribute exchange mechanism to exchange ETS information between the peers. In this exchange, each peer device sends its ETS configuration via the “configuration” ETS TLV and recommended ETS settings for the peer using the “recommend” ETS TLV. Both the configuration and recommendation ETS TLVs are implemented for Dell EMC Networking switches.

The peer ETS TLVs are stored in the DCBX database and are accessible using show commands.

The Application Priority TLV is accepted from auto-upstream devices and propagated to auto-downstream devices. In addition, if iSCSI CoS is enabled, an additional entry in the Application Priority TLV is added as discussed in the iSCSI section.

**Data Center Bridging Exchange Protocol Main Objective**

The DCBX protocol implementation conforms to the IEEE 802.1Qaz specification with some exceptions. To be interoperable with legacy industry implementations of DCBX protocol, a hybrid model is used to support both the IEEE version of DCBX and legacy DCBX versions. The hybrid version of the DCBX conforms to all aspects of the legacy standards to the degree necessary to support interoperability with a wide variety of FCoE capable switches.

The main objective of DCBX is to perform the following operations:

- Discovery of DCB capability in a peer
  DCBX is used to learn about the capabilities of the peer device. It is a means to determine if the peer device supports a particular feature such as PFC.
- DCB feature misconfiguration detection
DCBX can be used to detect misconfiguration of a feature between the peers on a link. Misconfiguration detection is feature-specific because some features may allow asymmetric configuration.

- Peer configuration of DCB features

DCBX can be used by a device to perform configuration of DCB features in its peer device if the peer device is willing to accept configuration.

**Interoperability with IEEE DCBX**

The Dell EMC Networking switch automatically detects if a peer is operating with either of the two CEE DCBX versions or the IEEE standard DCBX version. This is the default mode. DCBX can also be configured to manually select one of the legacy versions or IEEE standard mode. In auto-detect mode, the switch starts operating in IEEE DCBX mode on a port and if it detects a legacy DCBX device based on the OUI of the organization TLV, then the switch changes its DCBX mode on that port to support the version detected. There is no time out mechanism to move back to IEEE mode. Once the DCBX peer times out, multiple peers are detected, the link is reset (link down/up) or as commanded by the operator, DCBX resets its operational mode to IEEE.

The interaction between DCBX component and other components remains the same irrespective of the operational mode it is executing. For instance, DCBX component interacts with PFC to get needed information to pack the TLVs to be sent out on the interface. Based on the operational control mode of the port, DCBX packs it in the proper frame format.

**Port Roles**

Each port’s behavior is dependent on the operational mode of that port and of other ports in the stack. The port mode is a DCBX configuration item that is passed to the DCBX clients to control the processing of their configuration information. There are four port roles:

1. Manual
2. Auto-Upstream
3. Auto-Downstream
4. Configuration Source
**Manual**

Ports operating in the Manual role do not have their configuration affected by peer devices or by internal propagation of configuration. These ports have their operational mode and TC and bandwidth information specified explicitly by the operator. These ports will advertise their configuration to their peer if DCBX is enabled on that port. Incompatible peer configurations will be logged and counted with an error counter.

The default operating mode for each port is Manual for Dell EMC Networking releases; however, customer platforms may change the default mode for selected ports to either Auto-Upstream or Auto-Downstream mode. An example of this would be a blade switch that needed to support touchless configuration and has certain ports that are upstream ports and other ports that are downstream ports. A port that is set to manual mode sets the willing bit for DCBX client TLVs to false. Manually configured ports never internally propagate or accept internal or external configuration from other ports. Manually configured ports may notify the operator of incompatible configurations if client configuration exchange over DCBX is enabled. Manually configured ports are always operationally enabled for DCBX clients, regardless of whether DCBX is enabled.

**Auto-Upstream**

Advertises a configuration, but is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports as well as receive configuration propagated internally by other auto-upstream ports. The local operational parameters for PFC and ETS, if any, are overridden with the negotiated configuration. Specifically, the willing parameter is enabled on the port and the recommendation TLV is sent to the peer and processed if received locally. The first auto-upstream port to successfully accept a compatible configuration becomes the configuration source. The configuration source propagates its configuration to other auto-upstream and auto-downstream ports. Only the configuration source may propagate configuration to other ports internally. Auto-upstream ports that receive internally propagated information ignore their local configuration and utilize the internally propagated information.

Peer configurations received on auto-upstream ports other than the configuration source result in one of two possibilities.
1. If the configuration is compatible with the configuration source, then the DCBX client becomes operationally active on the upstream port.

2. If the configuration is not compatible with the configuration source, then a message is logged indicating an incompatible configuration, an error counter is incremented, and the DCBX client is operationally disabled on the port. The expectation is that the network administrator configures the upstream devices appropriately so that all such devices advertise a compatible configuration.

**Auto-Downstream**

An auto-downstream port advertises a configuration but is not willing to accept one from the link partner. However, the port will accept a configuration propagated internally by the configuration source. The local operational parameters for PFC and ETS, if any, are overridden with the negotiated configuration. Specifically, the willing parameter is disabled on auto-downstream ports. By default, auto-downstream ports have the recommendation TLV parameter enabled. Auto-downstream ports that receive internally propagated information ignore their local configuration and utilize the internally propagated operational information.

**Configuration Source**

In this role, the port has been manually selected to be the configuration source. Configuration received over this port is propagated to the other auto-configuration ports; however, no automatic election of a new configuration source port is allowed. Only one port can be configured as the configuration source. The local configuration parameters for PFC and ETS, if any, are overridden with the received configuration. Events that cause selection of a new configuration source are ignored. The configuration received over the configuration source port is maintained until cleared by the operator (set the port to the manual role). FIP snooping must be enabled to set a port to configuration source. For interfaces configured in a port-channel for which it is desirable to receive configuration information, it is strongly recommended that the auto-up setting be used on the Ethernet interfaces in the port channel in preference to the configuration source parameter.
**Configuration Source Port Selection Process**

When an auto-upstream or auto-downstream port receives a configuration from a peer, the DCBX client first checks if there is an active configuration source. If there is a configuration source already selected, the received configuration is checked against the local port operational values as received from the configuration source, and if compatible, the client marks the port as operationally enabled. If the configuration received from the peer is determined to not be compatible, a message is logged, an error counter is incremented and the DCBX clients become operationally disabled on the port. The port continues to keep link up and exchanges DCBX packets. If a compatible configuration is later received, the DCBX clients will become operationally enabled.

If there is no configuration source, a port may elect itself as the configuration source on a first-come, first-serve basis from the set of eligible ports. A port is eligible to become the configuration source if:

- No other port is the configuration source.
- The port role is auto-upstream.
- The port is enabled with link up and DCBX enabled.
- The port has negotiated a DCBX relationship with the partner.
- The switch is capable of supporting the received configuration values, either directly or by translating the values into an equivalent configuration.

N.B. Whether or not the peer configuration is compatible with the configured values is NOT considered.

The newly elected configuration source propagates DCBX client information to the other ports and is internally marked as being the port over which configuration has been received. Configuration changes received from the peer over the configuration source port are propagated to the other auto-configuration ports. Ports receiving auto-configuration information from the configuration source ignore their current settings and utilize the configuration source information.

When a configuration source is selected, local ETS and PFC configuration for all auto-up, auto-down and config-source ports is overridden by the configuration received from the configuration source.
In order to reduce flapping of configuration information, if the configuration source port is disabled, disconnected or loses LLDP connectivity, the system clears the selection of configuration source port (if not manually selected) and enables the willing bit on all auto-upstream ports. The configuration on the auto-configuration ports is not cleared (configuration holdover). If the user wishes to clear the configuration on the system in this scenario, the user can put the configuration source port into manual mode.

When a new port is selected as configuration source, it is marked as the configuration source, the DCBX configuration is refreshed on all auto-configuration ports and each port may begin configuration negotiation with their peer again (if any information has changed).

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Data Center Bridging Capability Exchange Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>datacenter-bridging</td>
</tr>
<tr>
<td>lldp dcbx version</td>
</tr>
<tr>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enhanced Transmission Selection Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>classofservice traffic-class-group</td>
</tr>
<tr>
<td>traffic-class-group max-bandwidth</td>
</tr>
<tr>
<td>traffic-class-group min-bandwidth</td>
</tr>
<tr>
<td>traffic-class-group strict</td>
</tr>
</tbody>
</table>

**Data Center Bridging Capability Exchange Commands**

**datacenter-bridging**

Use the `datacenter-bridging` command for an Ethernet interface in order to enter the DataCenterBridging mode. Priority-Flow-Control is configurable from within the DataCenterBridging mode.
Syntax

datacenter-bridging

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

NOTE: This command is only available on N40xx series switches.

Datacenter bridging mode is only available on Ethernet interfaces, not on port-channel interfaces. To ensure proper operation, users must configure all Ethernet interfaces in a port channel to have the same data-center bridging configuration.

Example

console#config
console(config)#interface range ethernet all
console(config-if)#datacenter-bridging
console(config-if-dcb)#priority-flow-control mode on
console(config-if-dcb)#priority-flow-control priority 1 no-drop

lldp dcbx version

Use the **lldp dcbx version** command in Global Configuration mode to configure the administrative version for the Data Center Bridging Capability Exchange (DCBX) protocol. This command enables the switch to support a specific version of the DCBX protocol or to detect the peer version and match it. DCBX can be configured to operate in IEEE mode or CEE mode or CIN mode. In auto mode, version detection is based on the peer device DCBX version. The switch operates in either IEEE or one of the legacy modes on each interface.

NOTE: CIN is Cisco Intel Nuova DCBX (version 1.0). CEE is converged enhanced ethernet DCBX (version 1.06).

Use the **no** form of the command to reset the dcbx version to the default value of auto.
Syntax
lldp dcbx version {auto | cin | cee | ieee}
no lldp dcbx version

- auto—Automatically select the version based on the peer response.
- CIN—Force the mode to Cisco-Intel-Nuova. (DCBX 1.0)
- CEE—Force the mode to CEE (DCBX 1.06)
- IEEE—Force the mode to IEEE 802.1Qaz

Default Configuration
The default version is auto.

Command Mode
Global Config

User Guidelines
NOTE: This command is only available on N40xx series switches.

In auto mode, the switch will attempt to jump start the exchange by sending an IEEE frame, followed by a CEE frame followed by a CIN frame. The switch will parse the received response and immediately switch to the peer version. Because LLDP is a link local protocol, it cannot be configured on a port channel or VLAN interface. It is recommended that all ports configured in a port channel utilize the same LLDP configuration.

Example
The following example configures the switch to use CEE DCBX.

```
s1(config)#lldp dcbx version cee
```

LLdp dcbx port-role

Use the `lldp dcbx port-role` command in Interface Configuration mode to configure the port role to manual, auto-upstream, auto-downstream and configuration source. The default port role is manual.
Syntax
lldp dcbx port-role {auto-up | auto-down | manual | configuration-source}

- **Manual**—Ports operating in the ‘Manual’ role do not have their configuration affected by peer devices or by internal propagation of configuration. These ports will advertise their configuration to their peer if DCBX is enabled on that port. The willing bit is set to disabled on manual role ports.

- **Auto-up**—Advertises a configuration, but is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports as well as receive configuration propagated internally by other auto-upstream ports. These ports have the willing bit enabled. These ports should be connected to FCFs.

- **Auto-down**—Advertises a configuration but is not willing to accept one from the link partner. However, the port will accept a configuration propagated internally by the configuration source. These ports have the willing bit set to disabled. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF.

- **Configuration Source**—In this role, the port has been manually selected to be the configuration source. Configuration received over this port is used to configure the switch and is propagated to the other auto-configuration ports. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF. These ports have the willing bit enabled.

**Default Configuration**
The default port role is manual.

**Command Mode**
Interface Config

**User Guidelines**
NOTE: This command is only available on N40xx series switches.
In order to reduce configuration flapping, ports that obtain configuration information from a configuration source port will maintain that configuration for 2x the LLDP time out, even if the configuration source port becomes operationally disabled.

**Examples**

This example configures an FCF facing port:

```
console(config-if-Tel/1/1)#lldp dcbx port-role auto-up
```

This example configures an FCoE host facing port:

```
console(config-if-Tel/1/1)#lldp dcbx port-role auto-down
```

**show lldp tlv-select**

Use the `lldp tlv-select` command to display the Traffic Class to Traffic Class Group mapping.

**Syntax**

```
show lldp tlv-select interface [all | interface-id]
```

- `interface-id`—A valid Ethernet interface specifier
- `all`—All interfaces

**Default Configuration**

The default is to show the per interface TLV configuration.

**Command Mode**

Privileged Exec

**User Guidelines**

NOTE: This command is only available on N40xx series switches.

This command has no user guidelines.

**Examples**

```
console# show lldp tlv-select interface Tel/0/1
Interface    ETS Config  ETS Recommend  PFC  App Priority QCN
------------ ----------  -------------  ---  ------------ ---
tel/0/1      Yes         No             Yes  No           Yes
```
show lldp dcbx

Use the `show lldp dcbx` command to display the Traffic Class to Traffic Class Group mapping.

**Syntax**

```
show lldp dcbx [interface [all|interface-id detail|status]]
```

- `interface-id`—A valid Ethernet interface specifier.
- `all`—All interfaces.
- `detail`—Display detailed DCBX information.
- `status`—Display a status summary.

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec

**User Guidelines**

NOTE: This command is only available on N40xx series switches.

This command has no user guidelines.

**Example #1**

DCBX Status:

```
console# show lldp dcbx interface all status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Role</th>
<th>Version</th>
<th>Rx</th>
<th>Tx</th>
<th>Errors</th>
<th>Dscr</th>
<th>Dscr</th>
</tr>
</thead>
<tbody>
<tr>
<td>te1/0/1</td>
<td>Enabled</td>
<td>Auto-up</td>
<td>CEE 1.06</td>
<td>Yes</td>
<td>32</td>
<td>37</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>te1/0/2</td>
<td>Enabled</td>
<td>Auto-up</td>
<td>IEEE</td>
<td>32</td>
<td>37</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Example #2

DCBX not enabled:

```
console# show lldp dcbx interface te1/0/1
Interface te1/0/1
  DCBX Admin Status:                   Disabled
  Configured DCBX Version:              Auto-detect
  Peer DCBX Version:
  Peer MAC:
  Peer Description:
  Auto-configuration Port Role:        Manual
  Peer Is Configuration Source:        False

Error Counters:
  ETS Incompatible Configuration: 0
  PFC Incompatible Configuration: 0
  Disappearing Neighbor:          0
  Multiple Neighbors Detected:    0
```

Example #3

DCBX enabled – legacy device (CIN/CEE):

```
console# show lldp dcbx interface te1/0/1
Interface te1/0/1
  DCBX Admin Status:                   Enabled
  Configured Version:                  Auto-detect
  Peer DCBX Version:                CIN Version 1.0
  Peer MAC: 00:23:24:A4:21:03
  Peer Description:                    Cisco Nexus 5020 IOS Version 5.00
  Auto-configuration Port Role:        Auto-downstream
  Peer Is Configuration Source:        False

Local Configuration:

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Version</th>
<th>En/Will/Adv</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFC(3)</td>
<td>000</td>
<td>000</td>
<td>Y/Y/Y</td>
</tr>
<tr>
<td>PG(2)</td>
<td>000</td>
<td>000</td>
<td>Y/Y/Y</td>
</tr>
<tr>
<td>APP(4)</td>
<td>000</td>
<td>000</td>
<td>Y/Y/Y</td>
</tr>
</tbody>
</table>

Number of TCs Supported: 3
**Priority Group Id:** 0:00 1:01 2:02 3:03 4:04 5:05 6:06 7:07  
**PG Percentage (%):** 0:12 1:10 2:12 3:00 4:00 5:66 6:00 7:00  
**Strict Priority:** 0:0 1:2 2:0 3:0 4:0 5:0 6:0 7:0  
**PFC Enable Vector:** 0:0 1:1 2:0 3:0 4:0 5:0 6:0 7:0  

**Peer Configuration:**

**Operation version:** 00  **Max version:** 00  **Seq no:** 23  **Ack no:** 22  

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Version</th>
<th>En/Will/Err</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFC(3)</td>
<td>000</td>
<td>000/000</td>
<td>Y/N/N</td>
</tr>
<tr>
<td>PG(2)</td>
<td>000</td>
<td>000/000</td>
<td>Y/N/N</td>
</tr>
<tr>
<td>APP(4)</td>
<td>000</td>
<td>000/000</td>
<td>Y/N/N</td>
</tr>
</tbody>
</table>

**Number of TCs Supported:** 3  
**Priority Group Id:** 0:00 1:01 2:02 3:03 4:04 5:05 6:06 7:07  
**PG Percentage (%):** 0:0 1:10 2:12 3:00 4:00 5:78 6:00 7:00  
**PFC Enable Vector:** 0:0 1:1 2:0 3:0 4:0 5:1 6:0 7:0  

**Application Priority (TX Enabled)**  

<table>
<thead>
<tr>
<th>Type</th>
<th>Application</th>
<th>Priority</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>FC0E</td>
<td>3</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCP/SCTP</td>
<td>860</td>
<td>4</td>
<td>Disabled</td>
</tr>
<tr>
<td>TCP/SCTP</td>
<td>3260</td>
<td>4</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Error Counters:**  
**ETS Incompatible Configuration:** 0  
**PFC Incompatible Configuration:** 0  
**Disappearing Neighbor:** 0  
**Multiple Neighbors Detected:** 0  

**Example #4**

**DCBX enabled – IEEE device (DCBX Version Forced):**

```bash
console# show lldp dcbx interface te1/0/1
```

**Interface te1/0/1**

<table>
<thead>
<tr>
<th>DCBX Admin Status:</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured DCBX Version:</td>
<td>CIN 1.0</td>
</tr>
<tr>
<td>Peer DCBX Version:</td>
<td>CEE 1.6</td>
</tr>
<tr>
<td>Peer MAC: 00:23:24:A4:21:03</td>
<td></td>
</tr>
<tr>
<td>Peer Description:</td>
<td>Cisco Nexus 5020 IOS Version 5.00</td>
</tr>
<tr>
<td>Auto-configuration Port Role:</td>
<td>Auto-upstream</td>
</tr>
<tr>
<td>Peer Is Configuration Source:</td>
<td>True</td>
</tr>
</tbody>
</table>
**Example #5**

DCBX enabled – detailed view:

```
console# show lldp dcbx interface te1/0/1 detail

Interface te1/0/1
  DCBX Admin Status:       Enabled
  Configured Version:      Auto-detect
  Auto-configuration Port Role: Configuration Source
  Peer Is Configuration Source: True

PFC Capability (TX Enabled)
  Willing: True  MBC: False  Max PFC classes supported: 3
  PFC Enable Vector:  0:0 1:1 2:0 3:0 4:0 5:1 6:0 7:0

ETS Configuration (TX Enabled)
  Willing: True  Credit Shaper: True  Traffic Classes Supported: 8
  Priority Assignment:  0:0 1:1 2:2 3:3 4:4 5:5 6:6 7:7
  Traffic Class Bandwidth (%):  0:00 1:10 2:12 3:00 4:00 5:78 6:00 7:00
  Traffic Selection Algorithm:  0:0 1:1 2:2 3:0 4:0 5:3 6:0 7:0

Peer DCBX Version:     CEE 1.6
Peer Description:      Cisco Nexus 5020 IOS Version 5.00
Peer MAC:              00:23:24:A4:21:03
Peer PFC Capability:
  Willing: False  MBC: False  Max PFC classes supported: 3
  PFC Enable Vector:  0:0 1:1 2:0 3:0 4:0 5:1 6:0 7:0

Peer ETS Configuration:
  Willing: False  Peer ETS Detected: True  Credit Shaper: True
  Traffic Classes Supported:  8
  Priority Assignment:  0:0 1:1 2:1 3:0 4:0 5:1 6:0 7:0
  Traffic Class Bandwidth:  0:00 1:10 2:12 3:00 4:00 5:78 6:00 7:00
  Traffic Selection Algorithm:  0:0 1:1 2:2 3:0 4:0 5:3 6:0 7:0

Peer Application Priority
  Type     Application     Priority
  ------------------------------
```

Error Counters:
ETS Incompatible Configuration: 7
PFC Incompatible Configuration: 0
Disappearing Neighbor: 0
Multiple Neighbors Detected: 0
Enhanced Transmission Selection (ETS) Commands

NOTE: Enhanced Transmission Selection commands are only supported on N4000 series switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.

classofservice traffic-class-group

This command maps the internal Traffic Class to an internal Traffic Class Group (TCG). The Traffic Class can range from 0-6, although the actual number of available traffic classes depends on the platform.

Use the no form of this command to return system (Global Configuration mode) or interface (Interface Configuration mode) to the default mapping.

Syntax

classofservice traffic-class-group trafficclass traffic class group

no classofservice traffic-class-group

- trafficclass—The selected traffic class. Range is 0-6.
- trafficclassgroup—The selected group. Range 0-2.

Default Configuration

By default, all the traffic classes are mapped to TCG 0. In the default configuration, all the Traffic Classes are grouped as one Traffic Class Group and TCG0 is configured as weighted round robin.

Command Mode

Global Config, Interface Configuration modes

User Guidelines

NOTE: This command is only available on N40xx series switches.
For a given Traffic Class, a value specified in Interface Configuration mode only affects a single interface, whereas a change in Global Configuration mode is applied to all interfaces. The Interface Configuration mode command is only available on platforms that support independent per-port class of service mappings. Ports that are configured to use the DCBX auto-configuration roles (auto-up or auto-down) have their ETS settings overridden. Only ports configured as DCBX manual role utilize the configured ETS settings.

It is recommended that all strict priority traffic classes be mapped to a single TCG.

Internally, frames are selected for transmission from the strict priority TCGs first, then, once the constraints of the TCGs are satisfied, frames from the WRR TCGs are selected for transmission. For example, grouping strict priority assignments into TCG 1 and weighted assignments into TCG 0 will result in all frames of the highest priority in TCG 1 being transmitted first, then the next lower priority, et. seq. until no frames remain for transmission in TCG 1. Then the scheduler will process frames from TCG 0, giving them appropriate treatment based upon the weights, minimum bandwidth and maximum bandwidth constraints.

Traffic class group 7 is reserved by the system for internal use.

**Example**

The following example demonstrates how to globally map priorities 1 and 2 to TCG 1.

```sh
console(config)# classofservice traffic-class-group 1 1
console(config)# classofservice traffic-class-group 2 1
```

**traffic-class-group max-bandwidth**

Use this command in Global Config or Interface Configuration mode to specify the maximum transmission bandwidth limit for each TCG as a percentage of the interface rate. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bound.

**Syntax**

```
traffic-class-group max-bandwidth bw-0 bw-1 … bw-n
```
no traffic-class-group max-bandwidth
  • bw-0..7—The maximum percentage bandwidth to be transmitted by the TCG. Range 0 to 100.

Default Configuration
The default maximum bandwidth for all TCGs is 0% (unlimited).

Command Mode
Global Config, Interface Configuration modes

User Guidelines
NOTE: This command is only available on N40xx series switches.

This command specified in Interface Configuration mode only affects a single interface; whereas, the Global Configuration mode setting is applied to all interfaces. Interface configuration overrides the global configuration on the designated interface. The Interface Configuration mode command is only available on platforms that support independent per-port class of service queue configuration.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command and each is independent of the others. The number n is platform dependent and corresponds to the number of supported traffic classes groups. The default maximum bandwidth value for each TCG is 0, meaning no upper limit is enforced, which allows the TCG queue to consume any available non-guaranteed bandwidth of the interface.

If a non-zero value is specified for any bw-x maximum bandwidth parameter, it must not be less than the current minimum bandwidth value for the corresponding queue. A bw-x maximum bandwidth parameter value of 0 may be specified at any time without restriction.

The maximum bandwidth limits may be used with either a weighted or strict priority scheduling scheme. Note that a value of 0 (the default) implies an unrestricted upper transmission limit, which is similar to 100%, although there may be subtle operational differences depending on how the device handles a no limit case versus limit to 100%.
Example
The following example demonstrates how to limit the maximum bandwidth percentage for TCG 1 and 2 to 25% each.

console(config)# traffic-class-group max-bandwidth 50 25 25

traffic-class-group min-bandwidth

Use this command in Global Config or Interface Configuration mode to specify the minimum transmission bandwidth guaranteed for each TCG before processing frames from other TCGs on an interface.

Use the no form of the command to return the bandwidth reservations to the default values.

Syntax

traffic-class-group min-bandwidth bw-0 bw-1 … bw-n
no traffic-class-group min-bandwidth

• bw-0..7—The maximum percentage bandwidth to be transmitted by the TCG. Range 0 to 100.

Default Configuration

The default minimum bandwidth for all TCGs is 0% (no minimum guarantee).

Command Mode

Global Configuration mode, Interface Configuration mode

User Guidelines

NOTE: This command is only available on N40xx series switches.

This command specified in Interface Configuration mode only affects a single interface, whereas the Global Configuration mode setting is applied to all interfaces. The Interface Configuration mode command is only available on the N4000 series switches.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The default minimum bandwidth
value for each TCG is 0, meaning no bandwidth is guaranteed (best effort). In order to better accommodate bursty traffic, it is recommended that the sum of the minimum bandwidths configured be much less than 100%.

If the value of any bw-x minimum bandwidth parameter is specified as greater than the current maximum bandwidth value for the corresponding TCG, then its corresponding maximum bandwidth automatically increases the maximum to the same value. Min-bandwidth may be configured manually by the operator on manual and auto-configuration ports. If the port is an auto-configuration port, the weights received via ETS TLVs are taken into account by the scheduler along with the min-bandwidth parameters supplied by the operator.

Refer to the `cos-queue min-bandwidth` command for information regarding scheduling frame for transmission across TCGs.

**Example**

The following example demonstrates how to reserve the minimum bandwidth percentage for TCG 1 and 2 to 25% each and reserve the remaining bandwidth for TCG 0.

```
console(config)# traffic-class-group min-bandwidth 50 25 25
```

**traffic-class-group strict**

Use this command in Global Config or Interface Configuration mode to activate the strict priority scheduler mode for each specified TCG.

Use the `no` form of the command to return the TCGs to the default weighted scheduler mode.

**Syntax**

```
traffic-class-group strict tcg-id [tcg-id ... tcg-id]
no traffic-class-group strict
```

- **tcg-id**—The TCG identifier. Range is 0 to 2

**Default Configuration**

The default scheduling mode for all TCGs is weighted scheduling.
**Command Mode**

Global Configuration mode, Interface Configuration mode

**User Guidelines**

NOTE: This command is only available on N40xx series switches.

This command specified in Interface Configuration mode only affects a single interface, whereas the Global Configuration mode setting is applied to all interfaces. The Interface Configuration mode command is only available on platforms that support independent per-port class of service queue configuration.

At least one, but no more than \( n \), tcg-id values are specified with this command. Duplicate \texttt{tcg-id} values are ignored. Each \texttt{tcg-id} value ranges from 0 to \((n-1)\), where \( n \) is the total number of TCG supported per interface. The number \( n \) is platform dependent and corresponds to the number of supported Traffic Class Groups.

When strict priority scheduling is used for a TCG, the minimum bandwidth setting for the TCG is ignored and packets are scheduled for transmission as soon as they arrive. A maximum bandwidth setting for the queue, if configured, serves to limit the outbound transmission rate of a strict priority TCG queue so that it does not consume the entire capacity of the interface. If multiple TCGs on the same interface are configured for strict priority mode, the method of handling their packet transmission, gives preference among the strict priority TCGs to the one with the highest \texttt{tcg-id}. Strict priority or weighted scheduling may be configured manually or via DCBX using the ETS TLVs.

**Example**

The following example demonstrates how to set TCGs 1 and 2 to strict priority scheduling.

```console
console(config)# traffic-class-group strict 1 2
```
**traffic-class-group weight**

Use the traffic-class-group weight command in Global Config or Interface Configuration mode to specify the scheduling weight for each TCG. The scheduler attempts to balance the traffic selected for transmission from the TCGs such that, when the switch is congested, traffic is selected from the round robin configured TCGs in proportion to their weights.

Use the `no` form of the command to return the TCGs to the default weighted scheduler mode.

**Syntax**

```
traffic-class-group weight wp-0 wp-1 wp-2
no traffic-class-group strict
```

- `wp-n`—The weight percentage. Range 0 to 100.

**Default Configuration**

The default weight is in the ratio of 1:2:3 for TCG0:TCG1:TCG2 (100%:0%:0%).

**Command Mode**

Global Configuration mode, Interface Configuration mode

**User Guidelines**

**NOTE:** This command is only available on N40xx series switches.

This command specified in Interface Configuration mode only affects a single interface, whereas the Global Configuration mode setting is applied to all interfaces. The Interface Configuration mode command is only available on platforms that support independent per-port class of service queue configuration.

The weight percentage is not considered for Traffic Class Groups that are configured for strict priority scheduling. Auto-configuration ports utilize the weights received from the auto-configuration source but do not alter the manual settings. Manually configured ports enabled for DCBX transmit the manually configured weights in the TC Bandwidth table in the ETS TLVs.
Each **wp-x** (weight percentage) value is a percentage that ranges from 0 to 100 in increments of 1. All **n** bandwidth values must be specified with this command, and their combined sum must equal 100%. The weight percentage may be configured manually or via the DCBX protocol using the ETS TLVs.

**Example**

The following example demonstrates how to set TCG 0 to 50% weight and TCG 1 to 50%.

```
console(config)# traffic-class-group weight 50 5 0
```

**show classofservice traffic-class-group**

Use the `show classofservice traffic-class-group` command to display the Traffic Class to Traffic Class Group mapping.

**Syntax**

```
show classofservice traffic-class-group [interface-id]
```

- **interface-id**—The ID for the interface for which to display information.

**Default Configuration**

The default is to show the global traffic class to group mapping.

**Command Mode**

Privileged Exec mode

**User Guidelines**

NOTE: This command is only available on N40xx series switches.

The interface-id parameter is optional. If specified, the TCG mapping table of the interface is displayed. If omitted, the global configuration settings are displayed (these may have been subsequently overridden by per-port configuration).

Traffic class group 7 is reserved by the system and is not shown.

Auto-configuration ports utilize the traffic class group mappings received from the auto-configuration source. Manually configured ports enabled for DCBX transmit the traffic class groups in the ETS TLVs.
Example

The following example demonstrates how to display the global traffic class to group mappings:

```
s1# show classofservice traffic-class-group
Traffic Class     Traffic Class Group
-------------    ---------------------
  0               0
  1               1
  2               1
  3               1
  4               2
  5               1
  6               1
```

**show interfaces traffic**

Use the `show interfaces traffic` command to display traffic information.

**Syntax**

```
show interfaces traffic [interface-id]
```

`interface-id`—A valid Ethernet interface specifier. Port-channels are not allowed with this command as the queuing and drops occur on the individual interfaces and not on the port channel.

**Default Configuration**

The default is to show the global traffic class group configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

The interface-id parameter is optional. The following information is displayed:
The above counters are cleared by the `clear counters` command. The queue sizes cannot be cleared as they are instantaneous.

**Example**

This example shows Gi1/0/1 is suffering from congestion (Tx Queue high) and is dropping packets, either due to WRED drops or due to exceeding the internal buffer limits.

<table>
<thead>
<tr>
<th>Intf</th>
<th>Congestion Drops (Pkts)</th>
<th>Tx Queue (Cells)</th>
<th>Rx Queue (Cells)</th>
<th>Color Drops (Pkts) Yellow</th>
<th>Red</th>
<th>WRED TX Queue (Pkts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>18981</td>
<td>132</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces traffic-class-group

Use the `show interfaces traffic-class-group` command to display the Traffic Class to Traffic Class Group mapping.

**Syntax**

`show interfaces traffic-class-group [interface-id]`

- `interface-id`—A valid Ethernet interface specifier.

**Default Configuration**

The default is to show the global traffic class group configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

NOTE: This command is only available on N40xx series switches.

The interface-id parameter is optional. If specified, the TCG mapping table of the interface is displayed. If omitted, the global configuration settings are displayed (these may have been subsequently overridden by per-port configuration).

The following information is displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.</td>
</tr>
<tr>
<td>Traffic Class Group</td>
<td>The traffic class Group identifier.</td>
</tr>
<tr>
<td>Min-Bandwidth</td>
<td>The minimum transmission bandwidth, expressed as a percentage. A value of 0 means bandwidth is not guaranteed. This is a configured value.</td>
</tr>
<tr>
<td>Max-Bandwidth</td>
<td>The maximum transmission bandwidth, expressed as a percentage. A value of 0 means no upper limit is enforced, so the queue may use any or all of the available bandwidth of the interface. This is a configured value.</td>
</tr>
</tbody>
</table>
Example

The following example demonstrates how to display the global traffic class group configuration:

```
sl1# show interfaces traffic-class-group
Global Configuration

TCG Id | Min. Bandwidth | Max Bandwidth | Scheduler | Weight Percentage
-------+---------------+--------------+-----------+-------------------
   0    |      0        |      0       | Strict    | 0
   1    |      0        |      0       | WDRR      | 50
   2    |      0        |      0       | WDRR      | 50
```
OpenFlow Commands

Dell EMC Networking N2000/N2100-ON/N3000/N3100/N4000 Series Switches

The OpenFlow feature configures the switch to be managed by a centralized OpenFlow Controller using the OpenFlow protocol. Openflow is not supported in a stacking environment. The OpenFlow agent has been validated with the Helium release of OpenDaylight (ODL).

Commands in this Section

This section explains the following commands:

- controller
- openflow
- hardware profile openflow
- passive
- ipv4 address
- protocol-version
- mode
- show openflow

controller

Use the controller command to configure a connection to an OpenFlow controller. Use the no form of the command to remove an OpenFlow controller connection.

Syntax

controller ipv4 ipv4-address [port port-number] security { none | ssl }

no controller ipv4 { ipv4-address [port port-number] | all }

- ipv4-address—The IPv4 address of the controller.
- port-number—The TCP port number used for the connection on the controller.
- security { none | ssl }—The security used for connection to the controller.
- all—Delete all OpenFlow controllers
Default Configuration
No controllers are configured by default.

Command Mode
OpenFlow Configuration

User Guidelines
If connection to the controller over an interface other than the OOB interface is desired, use the OpenFlow mode command prior to issuing this command. Issuing the mode command after a connection has been established drops the connection. The connections are then re-attempted over the new interface as specified by the mode command.

If the OOB interface is used to connect to the OpenFlow controllers, the controllers should be on the same subnet as the OOB interface.

When using the no form of the command, if no port number is given, all controller entries for the IP address are deleted.

If SSL is used, an SSL certificate should be downloaded using the copy command prior to configuring the controller.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported.

OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

Command History
Introduced in version 6.3.0.1 firmware.

Example
This example enables OpenFlow 1.3 on a switch and configures a connection the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security. A signed CA certificate, switch certificate, and switch private key should be downloaded to the switch using the copy command.

console(config)#openflow

WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.
Data Center Technology Commands

hardware profile openflow

Use the hardware profile openflow command to select the forwarding mode for the OpenFlow hybrid capability. Use the no form of the command to select the default forwarding capability.

Syntax

hardware profile openflow { full-match | layer2-match }

no hardware profile openflow

- full-match—Perform full matching when configured in OpenFlow 1.0 mode.
- layer2-match—Perform L2 matching when configured in OpenFlow 1.0 mode.

Default Configuration

By default, layer2 matching is performed.

Command Mode

Global Configuration

User Guidelines

This command configures the switch when operating in OpenFlow 1.0 mode. It has no effect when operating in OpenFlow 1.3 mode.

If the administrator changes the default hardware table for OpenFlow 1.0 and if the switch is currently operating in OpenFlow 1.0 variant then the OpenFlow feature is automatically disabled and re-enabled.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported. OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.
**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
The following example configures OpenFlow 1.0 full matching, configures a connection to the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security, and enables OpenFlow 1.0 on the switch.

```
console(config)#hardware profile openflow full-match
console(config)#openflow

WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.

console(config-of-switch)#controller ipv4 1.2.3.4 port 3435 security ssl
console(config-of-switch)#protocol-version 1.0
console(config-of-switch)#mode auto
console(config-of-switch)#exit
```

**ipv4 address**
Use the `ipv4 address` command to assign the IPv4 source address utilized for controller connections. Use the `no` form of the command to return the setting to the default.

**Syntax**

ipv4 address ipv4-address

no ipv4 address

- ipv4-address—The configured IPv4 address of the switch. A VLAN interface must exist with an identical address.

**Default Configuration**
By default, the switch selects an address automatically.

**Command Mode**
OpenFlow Configuration
**User Guidelines**

This command configures the switch with a static IPv4 address. The switch must be configured in static mode in order to use the configured static address.

Only IPv4 addresses are supported for OpenFlow controllers.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported.

OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This example configures an interface using VLAN 10 with IPv4 address 1.2.3.1, configures a connection to the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security and initiates the connection over the switch front panel interface. The local switch is configured with a static IP address after being configured into static address mode.

```bash
console(config)#vlan 10
console(config-vlan10)#interface vlan 10
console(config-if-vlan10)#ip address 1.2.3.1 255.255.0.0
console(config-if-vlan10)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport mode access
console(config-if-Gi1/0/1)#switchport access vlan 10
console(config)#openflow

WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.

console(config-of-switch)#controller ipv4 1.2.3.4 port 3435 security ssl
console(config-of-switch)#mode static
console(config-of-switch)#ipv4 address 1.2.3.1
console(config-of-switch)#exit
```
mode

Use the **mode** command to configure the selection of interfaces used to assign the IP address utilized for controller connections. Use the **no** form of the command to return the setting to the default.

**Syntax**

```bash
mode { auto | static | oob }
no mode
```

- **auto**—Automatically select the switch IP address
- **static**—Use the configured static IP address
- **oob**—Use the OOB interface IP address

**Default Configuration**

By default, the switch selects an IP address automatically (auto mode).

**Command Mode**

OpenFlow Configuration

**User Guidelines**

This command configures the switch to select an IP address from a particular type of interface. The selected IP address is used as the local end-point of the IP connections to the OpenFlow controllers.

The administrator can allow the switch to automatically assign an IP address to the OpenFlow feature or to specifically select which address should be used. The administrator can also direct the OpenFlow feature to always use the out-of-band interface.

When in auto mode, the switch selects an IP address from an interface in this order:

1. The loopback interfaces.
2. The routing interfaces.
3. The out-of-band interface.
Once the IP address is selected, it is used until the interface goes down or the OpenFlow feature is disabled or, in case of automatic address selection, a more preferred interface becomes available.

Only IPv4 addresses are supported for OpenFlow controllers.

Changing the mode causes the connections to controllers to be dropped, and if properly configured, re-established.

If the switch is configured in static mode, OpenFlow will remain operationally disabled until a static IPv4 address is configured, the IPv4 address matches exactly an IPv4 address on a VLAN interface, and the VLAN interface is operationally enabled.

If the OOB interface is manually selected as the OpenFlow IP address then the Open Flow feature becomes enabled immediately, even if there is no IP address assigned to the service port.

If the OOB interface is used to connect to the OpenFlow controllers, the controllers should be on the same subnet as the OOB interface.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported.

OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This example configures an interface using VLAN 10 with IPv4 address 1.2.3.1, configures a connection to the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security and initiates the connection over the switch front panel interface.

```
console(config)#vlan 10
console(config-vlan10)#interface vlan 10
console(config-if-vlan10)#ip address 1.2.3.1 255.255.0.0
console(config-if-vlan10)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport mode access
console(config-if-Gi1/0/1)#switchport access vlan 10

console(config)#openflow
```
WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.

```
console(config-of-switch)#controller ipv4 1.2.3.4 port 3435 security ssl
console(config-of-switch)#mode auto
console(config-of-switch)#exit
```

**openflow**

Use the `openflow` command to enable OpenFlow on the switch (if disabled) and enter into OpenFlow configuration mode. Use the `exit` command to return to Global Configuration mode.

**Syntax**

`openflow`

`no openflow`

**Default Configuration**

The OpenFlow capability is disabled by default. No controllers are configured by default. OpenFlow 1.3 mode is selected by default when OpenFlow is enabled. The OpenFlow protocol operates over the OOB interface by default.

**Command Mode**

Global Configuration

**User Guidelines**

When the OpenFlow feature is administratively disabled, the switch drops connections with the OpenFlow Controllers. The switch also purges all flows programmed by the controllers and removes the controller configuration.

Dell OpenFlow implements a true hybrid mode implementation of OpenFlow. Resources are allocated on a first-come first serve basis among the legacy switch UI and the OpenFlow controllers. No arbitration of resources is performed and conflicting actions are allowed.
OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported. OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This example enables OpenFlow 1.3 on a switch and configures a connection the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security.

```
console(config)#openflow

WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.

console(config-of-switch)#controller ipv4 1.2.3.4 port 3435 security ssl
```

**passive**

Use the `passive` command to set the switch to accept connections initiated by a controller.

**Syntax**

```
passive
no passive
```

**Default Configuration**

By default, the switch initiates the connection to the controllers.

**Command Mode**

OpenFlow Configuration
**User Guidelines**

This command configures the switch to accept a connection request from a controller. When passive mode is enabled, the switch accepts TCP connections to ports 6632 and 6633 respectively using any switch IP address. In this mode, the switch continues to attempt to initiate connections to configured controllers.

The OpenFlow component always initiates the SSL connections and does not accept SSL connections.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported. OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This example configures a connection to the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security and also configures the controller to accept TCP connections to the switch on port 6633.

```console
console(config)#openflow

WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.

console(config-of-switch)#controller ipv4 1.2.3.4 port 3435 security ssl
console(config-of-switch)#passive
console(config-of-switch)#mode auto
console(config-of-switch)#exit
```

**protocol-version**

Use the `protocol-version` command to select the version of the protocol in which to operate. Use the `no` form of the command to return the configuration to the default.
Syntax

protocol-version { 1.0 | 1.3 }
no protocol-version

- 1.0—Operate in OpenFlow 1.0 mode
- 1.3—Operate in OpenFlow 1.3 mode

Default Configuration

By default, the switch operates in OpenFlow 1.3 mode.

Command Mode

OpenFlow Configuration

User Guidelines

If the administrator changes the OpenFlow variant while the OpenFlow feature is enabled, the switch automatically disables and re-enables the OpenFlow feature causing all flows to be deleted and connections to the controllers to be dropped.

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported. OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

Command History

Introduced in version 6.3.0.1 firmware.

Example

This example enables OpenFlow 1.3 on a switch and configures a connection the controller at IPv4 address 1.2.3.4 TCP port 3435 using SSL security.

```
console(config)#openflow
WARNING! OpenFlow does not operate on stack members. Enable OpenFlow on stand-alone switches only.
```

```
console(config-of-switch)#protocol-version 1.3
console(config-of-switch)#mode auto
```
show openflow

Use the show openflow command to display OpenFlow configuration and status.

Syntax

show openflow [ switch controllers | switch flows | switch groups | switch tables ]

• switch controllers—Show information about configured controllers
• switch flows—Show information regarding flows
• switch groups—Show information regarding OpenFlow groups
• switch tables—Show information regarding the switch tables

Default Configuration

When invoked with no parameters, the show openflow command shows summary information regarding OpenFlow.

Command Mode

Privileged Exec and Global Configuration

User Guidelines

OpenFlow operates on the stack master only. Flows may not be configured on stack members. Failover to the stack standby unit is not supported. OpenFlow should only be enabled on stand-alone switches and should not be enabled on stacks of switches. This restriction is not enforced.

The command has the following output.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>The OpenFlow feature administrative mode set by the ‘openflow enable’ command.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>The operational status of the OpenFlow feature. Although the feature may be administratively enabled, it could be operationally disabled due to various reasons.</td>
</tr>
</tbody>
</table>
When the switch tables parameter is given, the following information is displayed:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Reason</td>
<td>If the OpenFlow feature is operationally disabled then this status shows the reason for the feature to be disabled.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IPv4 Address assigned to the feature. If the IP address is not assigned then the status is ‘None’.</td>
</tr>
<tr>
<td>IP Mode</td>
<td>IP mode assigned by the ‘openflow ip-mode’ command. The IP Mode can be “Auto”, “Static” or “ServicePort IP”</td>
</tr>
<tr>
<td>Static IP Address</td>
<td>Static IP address assigned by the ‘openflow static-ip-address’ command.</td>
</tr>
<tr>
<td>Network MTU</td>
<td>Maximum network packet size excluding the VLAN Tag.</td>
</tr>
<tr>
<td>OpenFlow Variant</td>
<td>OpenFlow Protocol Variant. The OpenFlow protocol can be “OpenFlow 1.0” or “OpenFlow 1.3”.</td>
</tr>
<tr>
<td>Default Table</td>
<td>The Hardware Table used as the target for flows installed by an OpenFlow 1.0 controller which is not enhanced to handle multiple hardware tables.</td>
</tr>
<tr>
<td>Passive Mode</td>
<td>The OpenFlow passive mode set by the ‘passive’ command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Table.</td>
<td>OpenFlow Table Identifier (0 – 255).</td>
</tr>
<tr>
<td>Flow Table Name.</td>
<td>The name of this table.</td>
</tr>
<tr>
<td>Flow Table Description.</td>
<td>A detailed description for this table.</td>
</tr>
<tr>
<td>Maximum Size.</td>
<td>Platform-defined maximum size for this flow table.</td>
</tr>
<tr>
<td>Number of Entries.</td>
<td>Total number of entries in this table. The count includes delete-pending entries.</td>
</tr>
<tr>
<td>Hardware Entries.</td>
<td>Number of entries currently inserted into the hardware.</td>
</tr>
<tr>
<td>Software-Only Entries.</td>
<td>Number of entries that are not installed in the hardware for any reason. This includes entries pending for insertion, entries that cannot be inserted due to missing interfaces and entries that cannot be inserted due to table-full condition.</td>
</tr>
</tbody>
</table>
When the switch groups parameter is given, the following information is displayed:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting for Space Entries</td>
<td>Number of entries that are not currently in the hardware because the attempt to insert the entry failed.</td>
</tr>
<tr>
<td>Flow Insertion Count.</td>
<td>Total number of flows that were added to this table since the switch powered up.</td>
</tr>
<tr>
<td>Flow Deletion Count.</td>
<td>Total number of flows that were deleted from this table since the switch powered up.</td>
</tr>
<tr>
<td>Insertion Failure Count.</td>
<td>Total number of hardware insertion attempts that were rejected due to lack of space since the switch powered up.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type</td>
<td>Type of Group: Indirect, All, Select, etc.</td>
</tr>
<tr>
<td>Group Id</td>
<td>Unique ID for the Group</td>
</tr>
<tr>
<td>Reference Count</td>
<td>This count indicates how many Select groups are referring to the current Indirect group. Reference Count is used only for Indirect groups.</td>
</tr>
<tr>
<td>Duration</td>
<td>The time since the group was created.</td>
</tr>
<tr>
<td>Bucket Count</td>
<td>Number of Buckets in the group.</td>
</tr>
<tr>
<td>Reference Group Id</td>
<td>References the Indirect group ID and used for Select group only.</td>
</tr>
</tbody>
</table>

When the switch flows parameter is selected, the following output is shown:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Type</td>
<td>Type of the Flow 1.0 Flow or Layer 2 Match etc.</td>
</tr>
<tr>
<td>Flow Table</td>
<td>The hardware table where the flow is installed.</td>
</tr>
<tr>
<td>Flow Priority</td>
<td>Priority of the flow versus other flows. Higher is better.</td>
</tr>
<tr>
<td>Match Criterion</td>
<td>The match criterion specified by the flow with the field and value like ingress port or ether type</td>
</tr>
<tr>
<td>Ingress Port</td>
<td>The port on which the flow is active.</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
Action | The action specified by the flow.
Duration | The time since the flow was created
Idle | The time since the flow was hit.
Installed in hardware | Shows 0 if for some reason the flow could not be added in the hardware.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This output shows an operationally disabled switch:

```
console#show openflow
Administrative Mode............................ Enable
Administrative Status.......................... Disabled
Disable Reason................................. No-Suitable-IP-Interface
IP Address..................................... None
IP Mode........................................ Auto
Static IP Address.............................. 10.1.1.1
Network MTU.................................... 1518
OpenFlow Variant............................... OpenFlow 1.0
Default Table.................................. layer-2-match
Passive Mode................................... Enable
```

This output shows an operationally enabled switch:

```
console#show openflow
Administrative Mode............................ Enable
Administrative Status.......................... Enabled
Disable Reason................................. None
IP Address..................................... 10.27.65.64
IP Mode........................................ Auto
Static IP Address.............................. 10.1.1.1
Network MTU.................................... 1518
OpenFlow Variant............................... OpenFlow 1.3
Default Table.................................. full-match
Passive Mode................................... Enable
```
This example shows the output for OpenFlow 1.0 using the `switch tables` parameter:

```
console#show openflow switch tables
Flow Table...............................1
Flow Table Name..........................Forwarding Database
Maximum Size.............................64
Number of Entries........................8
Hardware Entries.........................7
Software-Only Entries....................1
Waiting for Space Entries................0
Flow Insertion Count.....................1
Flow Deletion Count......................0
Insertion Failure Count..................0
Flow Table Description:
The forwarding database maps non-multicast MAC addresses and the ports on which these addresses are located.
```

This example shows the output for OpenFlow 1.3 using the `switch tables` parameter:

```
console#show openflow switch tables
Flow Table..................................... 60
Flow Table Name................................ Openflow 1.3
Maximum Size.................................1920
Number of Entries............................0
Hardware Entries............................0
Software-Only Entries.......................0
Waiting for Space Entries...................0
Flow Insertion Count........................0
Flow Deletion Count..........................0
Insertion Failure Count....................0
Flow Table Description..................... The Openflow 1.3 table matches on the packet layer-2 header, including DA-MAC, SA-MAC, VLAN, Vlan priority ether type; layer-3 header, including SRC-IP, DST-IP, IP protocol, IP-TOS; layer-4 header, including UDP/TCP source and dest port, ICMP type, and code; SRC-IPv6, DST_IPv6, IPv6 Flow Label, ECN, ICMPv6 type and code, source L4 Port for TCP / UDP / SCTP and input port including physical port and LAG port.
```
The following example shows the output when the switch groups parameter is given:

console#show openflow switch groups

Max Indirect Group Entries......................................... 1234
Current Indirect Group Entries in database......................... 123

Max All Group Entries.............................................. 1234
Current All Group Entries in database.............................. 123

Max Select Group Entries....................................... 1234
Current Select Group Entries in database.......................... 123

Group Id 12345678 type “Indirect”
=================================
Ref Count              1 : Duration            8 : Bucket Count     1
Bucket Entry List:
------------------
Bucket Index         25 : Output Port            1
Src MAC 00:00:00:00:00:AB : Dst MAC 00:00:00:00:00:CD
VLAN              101 : Reference Group Id    NA

Group Id 23456789 type “All”
==========================
Ref Count              NA : Duration            10 : Bucket Count    2
Bucket Entry List:
------------------
Bucket Index         26 : Output Port            2
Src MAC              NA : Dst MAC               NA
VLAN               102 : Reference Group Id   NA

Group Id 34567890 type “Select”
===============================
Ref Count              NA : Duration            10 : Bucket Count    3
Bucket Entry List:
------------------
Bucket Index         28 : Output Port           NA
Src MAC              NA : Dst MAC               NA
VLAN                 NA : Reference Group Id    12345678

Bucket Index         29 : Output Port           NA
Src MAC              NA : Dst MAC               NA
VLAN                 NA : Reference Group Id    12345678

Bucket Index         30 : Output Port           NA
Src MAC              NA : Dst MAC               NA
VLAN                 NA : Reference Group Id    12345678

This examples shows the output for OpenFlow 1.0 flows:

console#show openflow switch flows

Flow: 00000000       Type: “1DOT0”
Flow Table:         60           Priority:   1          Type: Untagged MAC
Match Criteria:
  Ingress port: Gi1/0/1       Egress Port:
  VLAN ID:            VLAN PCP:  EtherType: 0x0800
  Src MAC: 00:00:02:37:38:01  Src IP: 100.0.0.225    Src IP Port:
  Dst MAC: 00:00:18:37:22:01  Dst IP: 192.0.0.225    Dst IP Port:
  IP Protocol:       17            TOS:     32            DSCP: 8
  Action:            Drop
Duration (secs):   55       Idle (secs): 45        In HW:  Yes
Packet Count:   12321       HW Priority: 2131

This example shows the output for OpenFlow 1.3 flows:

console#show openflow switch flows

Flow: 00000000E1     Type: “1DOT3”
Match Criteria:
  Flow Table:       60           Priority:   10
  Ingress port: Gi1/0/1       Egress Port: Gi1/0/2
  VLAN ID:            VLAN PCP:  EtherType: 0x0800
  Src MAC: 00:00:02:37:38:01  Src IP: 100.0.0.225    Src IP Port: 1
  Dst MAC: 00:00:18:37:22:01  Dst IP: 192.0.0.225    Dst IP Port: 1
  IP Protocol:       17            TOS:     32            DSCP: 8
  Action:
Duration (secs): 5       Idle (secs): 2       In HW: Yes
Packet Count:  3       HW Priority: 65464

Flow 000001F9 type "1DOT3"

Match Criteria:
Flow Table: 60     Priority: 10
Ingress port: Gi1/0/1    Egress Port: Gi1/0/1
VLAN ID: 1     VLAN PFC: 1     EtherType: 0x0800
Src MAC: 00:00:02:37:38:01     Src IP: 100.0.1.249    Src IP Port: 1
Dst MAC: 00:00:18:37:22:01     Dst IP: 192.0.1.249    Dst IP Port: 1
IP Protocol: 17     TOS: 32     DSCP: 8

Action:
Duration (secs): 2       Idle (secs): 0       In HW: Yes
Packet Count:  9879       HW Priority: 786743
Priority Flow Control Commands

Dell EMC Networking N4000 Series Switches

Priority Flow Control (PFC) provides a means of pausing frames based on individual priorities on a single physical link. By pausing the congested priority or priorities independently, protocols that are highly loss sensitive can share the same link with traffic that has different loss tolerances with less congestion spreading than standard flow control. The priorities are differentiated by the priority field of the 802.1Q VLAN header. PFC is standardized by the IEEE 802.1Qbb specification.

PFC uses a new control packet defined in 802.1Qbb and therefore is not compatible with standard flow control. An interface that is configured for PFC will be automatically disabled for 802.3x flow control. When PFC is disabled on an interface, the flow control configuration for the interface becomes active. Any flow control frames received on a PFC configured interface are ignored.

Each priority is configured as either drop or no-drop. If a priority that is designated as no-drop is congested, the priority is paused. Drop priorities do not participate in pause. By default there are no priority classifications configured and PFC is not enabled.

While several no-drop priorities may be configured on a supporting system, the actual number of lossless priorities supported on a given system is a function of the switch chips packet buffer, the maximum supported MTU size, pause delay, the media type and the total number of ports enabled for lossless behavior. In order to guarantee lossless behavior, the switch chip must send a pause message prior to exhausting its available packet buffer and have sufficient buffer to absorb the delay. In order to accomplish this, it must reserve enough memory (headroom) to handle the max delay in processing the pause packet.

The maximum number of lossless priorities per interface is two. The headroom is only used for guaranteeing lossless behavior. There must be enough dynamic memory to handle the typical work load of the switch in addition to the headroom. With two no-drop priorities per interface and static allocations, there is only about 30 percent of the buffer space available for normal forwarding behavior.
The effective default behavior on an interface enabled for PFC without a no-drop priority is that no flow control (legacy or PFC) is enabled. If the user enables PFC but does not create any no-drop priorities, the interface will not be lossless.

Changing the drop and no-drop capabilities on an interface, either in flow control or priority flow control, may require that all ports briefly drop link. The priority to flow control group cannot be changed while traffic is running. When 802.3 link flow control is enabled, all priorities are mapped to a single flow control group. When Qbb is enabled, the priorities are each mapped into their own flow control group, where lossless groups have additional buffer to handle the round trip delay for flow control. In order to minimize the impact, the link will only be dropped when changing between 802.3 and Qbb.

**Commands in this Section**

This section explains the following commands:

- **Data Center Bridging Capability Exchange Commands**
  - `priority-flow-control priority`
  - `clear priority-flow-control statistics`
  - `show interfaces priority-flow-control`

- **priority-flow-control mode**

  Use the `priority-flow-control mode on` command in Datacenter-Bridging Configuration mode to enable Priority-Flow-Control (PFC) on an interface. To disable Priority-Flow-Control, use the `no` form of the command.

  **Syntax**

  - `priority-flow-control mode on`
  - `priority-flow-control mode off`
  - `no priority-flow-control mode`
    - `on`—Enable PFC on the interface.
    - `off`—Disable PFC on the interface.
**Default Configuration**
Priority-flow-control mode is off (disabled) by default.

**Command Mode**
Datacenter-Bridging Configuration mode

**User Guidelines**
NOTE: This command is only available on N40xx series switches.

PFC must be enabled before FIP snooping can operate over the interface. Use the no form of the command to return the mode to the default (off). VLAN tagging (trunk or general mode) must be enabled on the interface in order to carry the 802.1p value through the network. Additionally, the dot1 mapping to class-of-service must be set to one-to-one. Ports that are configured to use the DCBX auto-configuration roles (auto-up or auto-down) have their PFC settings overridden. Only ports configured as DCBX manual role utilize the configured PFC settings.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled. Because PFC is a link local protocol, it must be configured on all the interfaces aggregated in a port channel. Only configuring some of the ports in a port channel to use PFC will cause unexpected results and is not supported.

**Example**
The following example enables PFC on an interface.

```
S1(config)#interface tel/0/1
S1(config-if-Tel/0/1)#datacenter-bridging
S1(config-if-dcb)#priority-flow-control mode on
```

**priority-flow-control priority**

Use the `priority-flow-control priority` command in Datacenter-Bridging Configuration mode to enable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface. Up to two lossless priorities can be enabled on an interface.

Use the `no` form of the command to return all priorities to their default lossy behavior.
Syntax

priority-flow-control priority priority-list {drop | no-drop}

no priority-flow-control priority

• drop—Disable lossless behavior on the selected priorities.
• no-drop—Enable lossless behavior on the selected priorities.
• priority-list —A list of IEEE 802.1p priorities (up to two) which are to be configured as lossless.

Default Configuration

The default behavior for all priorities is tail-drop.

Command Mode

Datacenter-Bridging Configuration mode

User Guidelines

NOTE: This command is only available on N40xx series switches.

The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior. Ports that are configured to use the DCBX auto-configuration roles (auto-up or auto-down) have their PFC settings overridden. Only ports configured as DCBX manual role utilize the configured PFC settings.

Example

The following example sets priority 3 to no drop behavior.

s1(config)#interface te1/0/1
s1(config-if-Te1/0/1)#datacenter-bridging
s1(config-if-dcb)#priority-flow-control mode on
s1(config-if-dcb)#priority-flow-control priority 1 no-drop

clear priority-flow-control statistics

Use the clear priority-flow-control statistics command to clear all or interface Priority-Flow-Control statistics.
Syntax

clear priority-flow-control statistics [ethernet interface ]
  • interface — A valid Ethernet port.

Command Mode

Privileged Exec mode

User Guidelines

This command has no user guidelines.

Example #1

console#clear priority-flow-control statistics tengigabitethernet 1/0/1

Example #2

console#clear priority-flow-control statistics

show interfaces priority-flow-control

Use the show interfaces priority-flow-control command to display the global or interface priority flow control status and statistics.

Syntax

show interfaces interface-id priority-flow-control
  • interface-id—A valid Ethernet port identifier.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

NOTE: This command is only available on N40xx series switches.

This command has no user guidelines.

Examples

The following examples show the priority flow control status and statistics.

s1#show interfaces tengigabitethernet 1/0/1 priority-flow-control
Interface Detail: te1/0/1
PFC Configured State: Disabled
PFC Operational State: Enabled
Configured Drop Priorities: 2-7
Operational Drop Priorities: 2-7
Configured No-Drop Priorities: 0-1
Operational No-Drop Priorities: 0-1
Delay Allowance: 32456 bit times
Peer Configuration Compatible: True
Compatible Configuration Count: 3
Incompatible Configuration Count: 1

<table>
<thead>
<tr>
<th>Priority</th>
<th>Received PFC Frames</th>
<th>Transmitted PFC Frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

console#show interfaces priority-flow-control

<table>
<thead>
<tr>
<th>Port</th>
<th>Drop Priorities</th>
<th>No-Drop Priorities</th>
<th>Operational Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/1</td>
<td>0-2,4-7</td>
<td>3</td>
<td>Active</td>
</tr>
<tr>
<td>Te1/0/2</td>
<td>0-2,4-7</td>
<td>3</td>
<td>Active</td>
</tr>
<tr>
<td>Te1/0/3</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/4</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/5</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/6</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/7</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/8</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/9</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/10</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/11</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/12</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/13</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/14</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/15</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/16</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/17</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Te1/0/18</td>
<td>0-7</td>
<td></td>
<td>Inactive</td>
</tr>
<tr>
<td>Interface</td>
<td>Ports</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>Te1/0/19</td>
<td>0-7</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Te1/0/20</td>
<td>0-7</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Te1/0/21</td>
<td>0-7</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Te1/0/22</td>
<td>0-7</td>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Te1/0/23</td>
<td>0-2,4-7</td>
<td>3</td>
<td>Active</td>
</tr>
<tr>
<td>Te1/0/24</td>
<td>0-7</td>
<td>Inactive</td>
<td></td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

The sections that follow describe commands that conform to the OSI model’s Network Layer (Layer 3). Layer 3 Routing commands enable routing protocols to perform a series of exchanges over various data links to route data between any two nodes in a network. These commands define the addressing and routing structure of the Internet.

The Dell EMC N1100-ON Series switches do not support routing.

This section of the document contains the following Layer 3 topics:

<table>
<thead>
<tr>
<th>ARP Commands</th>
<th>Loopback Interface Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional Forwarding Detection Commands</td>
<td>IP Multicast Commands</td>
</tr>
<tr>
<td>Border Gateway Protocol Commands</td>
<td>IPv6 Multicast Commands</td>
</tr>
<tr>
<td>BGP Routing Policy</td>
<td>OSPF Commands</td>
</tr>
<tr>
<td>DVMRP Commands</td>
<td>OSPFv3 Commands</td>
</tr>
<tr>
<td>IGMP Commands</td>
<td>Router Discovery Protocol Commands</td>
</tr>
<tr>
<td>IGMP Commands</td>
<td>Routing Information Protocol Commands</td>
</tr>
<tr>
<td>IGMP Proxy Commands</td>
<td>Tunnel Interface Commands</td>
</tr>
<tr>
<td>IP Helper/DHCP Relay Commands</td>
<td>Virtual Router Commands</td>
</tr>
<tr>
<td>IP Routing Commands</td>
<td>Virtual Router Redundancy Protocol Commands</td>
</tr>
<tr>
<td>IPv6 Routing Commands</td>
<td></td>
</tr>
</tbody>
</table>

---
When a host has an IP packet to send on an Ethernet network, it must encapsulate the IP packet in an Ethernet frame. The Ethernet header requires a destination MAC address. If the destination IP address is on the same network as the sender, the sender uses the Address Resolution Protocol (ARP) to determine the MAC address associated with destination IP address. The network device broadcasts an ARP request, identifying the IP address for which it wants a corresponding MAC address. The IP address is called the target IP. If a device on the same physical network is configured with the target IP, it sends an ARP response giving its MAC address. This MAC address is called the target MAC.

If the destination IP address is not on the same network as the sender, the sender generally forwards the packet to a default gateway. The default gateway is a router that forwards the packet to its destination. The host may be configured with a default gateway or may dynamically learn a default gateway.

The router discovery protocol is one method that enables hosts to learn a default gateway. If a host does not know a default gateway, it can learn the first hop to the destination through proxy ARP. Proxy ARP (RFC 1027) is a technique used to make a machine physically located on one network appear to be logically part of a different physical network connected to the same router (may also be a firewall). Typically Proxy ARP hides a machine with a public IP address on a private network behind a router and still allows the machine to appear to be on the public network. The router proxies ARP requests and all network traffic to and from the hidden machine to make this fiction possible.

Proxy ARP is implemented by making a small change to a router's processing of ARP requests. Without proxy ARP, a router only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the router may also respond if it has a route to the target IP address. The router only responds if all next hops on its route to the destination are through interfaces other than the interface where the ARP request was received.
ARP Aging

Dynamic entries in the ARP cache are aged. When an entry for a neighbor router reaches its maximum age, the system sends an ARP request to the neighbor router to renew the entry. Entries for neighbor routers should remain in the ARP cache as long as the neighbor continues to respond to ARP requests. ARP cache entries for neighbor hosts are renewed more selectively. When an ARP cache entry for a neighbor host reaches its maximum age, the system checks if the cache entry has been used recently to forward data traffic. If so, the system sends an ARP request to the entry’s target IP address. If a response is received, the cache entry is retained and its age is reset to 0. By enabling the dynamic renew option, the system administrator can configure ARP to attempt to renew aged ARP entries regardless of their use for forwarding.

If the system learns a new ARP entry but the hardware does not have space to add the new ARP entry, the system attempts to remove entries that have not been used for forwarding recently. This action may create space for new entries in the hardware’s ARP table.

Commands in this Section

This section explains the following commands:

ARP

Use the arp command in Global Configuration mode to create an Address Resolution Protocol (ARP) entry. The arp command optionally creates a static ARP entry in the selected VRF. Use the no form of the command to remove the entry.
**Syntax**

**arp** [vrf vrf-name]ip-address hardware-address [ interface interface-id]

**no arp** ip-address

- **vrf-name**—The name of the VRF with which the ARP entry is to be associated. If no VRF is specified, the ARP entry is associated with the global ARP table.
- **ip-address** — IP address of a device on a subnet attached to an existing routing interface.
- **hardware-address** — A unicast MAC address for that device.
- **interface-id**—An optional IP unnumbered (VLAN) interface identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the vrf parameter.

The vrf parameter is only available on the N3000/N3100/N4000 switches.

The interface identifier is the identifier of the unnumbered interface, not the loopback interface from which the IP address is borrowed.

When adding a static ARP entry with an unnumbered interface, the ip address must match the mask of the unnumbered interface.

A static ARP entry is only installed if the IP address matches one of the local subnets. In case of unnumbered interfaces, static ARP entries created for the unnumbered-peer do not match any of the local subnets and cannot be resolved to an interface. By specifying the interface explicitly in the static ARP command, static ARP entries for unnumbered-peers can be configured.
**Example**

The following example creates an ARP entry consisting of an IP address and a MAC address.

```
console(config)#arp 192.168.1.2 00A2.64B3.A245
```

**arp cachesize**

Use the `arp cachesize` command in Global Configuration mode to configure the maximum number of entries in the ARP cache. To return the maximum number of ARP cache entries to the default value, use the `no` form of this command.

**Syntax**

```
arp cachesize integer
no arp cachesize
```

- `integer` — Maximum number of ARP entries in the cache. Use the `show sdm prefer` command to display the supported ARP cache size.

**Default Configuration**

The switch defaults to using the maximum allowed cache size.

**Command Mode**

Global Configuration mode

**User Guidelines**

The ARP cache size is dependent on the switching hardware used. The allowed range of values may be different from the example given below for a given switch model.

On VRF enabled switches, the ARP cache is shared among all VRF instances. Configuration of the cache size is shared among all VRF instances.

**Example**

The following example defines an arp cachesize of 1000.

```
console(config)#arp cachesize 1000
```
arp dynamicrenew

Use the `arp dynamicrenew` command in Global Configuration mode to enable the ARP component to automatically renew dynamic ARP entries when they age out. To disable the automatic renewal of dynamic ARP entries when they age out, use the `no` form of the command.

**Syntax**

```
arp dynamicrenew
no arp dynamicrenew
```

**Default Configuration**

The default state is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host is lost until the router receives an ARP reply from the host. Gateway entries, and entries for a neighbor router, are always renewed. The dynamic renew option only applies to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. If the ARP cache is full and a new host is learned, the oldest ARP cache entry is replaced with the new host entry. In a network where the number of potential neighbors is greater than the ARP
cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full. Dynamic renewal should be disabled in these networks.

**Example**

```
console#configure
console(config)#arp dynamicrenew
console(config)#no arp dynamicrenew
```

**arp purge**

Use the `arp purge` command to cause the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command. The `arp purge` command optionally removes a static ARP entry in the selected VRF.

**Syntax**

```
arp purge [vrf vrf-name] ip-address [ interface interface-id]
```

- vrf-name—The name of the VRF associated with the ARP entry which is to be removed. If no VRF is specified, the ARP entry is associated with the global ARP table is removed.
- ip-address — The IP address to be removed from ARP cache.
- interface-id—An optional IP unnumbered (VLAN) interface identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the vrf parameter.

The vrf parameter is only available on the N3000/N3100/N4000 switches.
The interface identifier is the identifier of the unnumbered interface, not the loopback interface from which the IP address is borrowed.

When the IP address does not uniquely identify an ARP entry, the interface must be given to uniquely identify the ARP entry. The interface may be numbered or unnumbered.

**Example**
The following example removes the specified IP address from arp cache.

```
console#arp purge 192.168.1.10
```

**arp resptime**

Use the `arp resptime` command in Global Configuration mode to configure the ARP request response time-out. To return the response time-out to the default value, use the no form of this command.

**Syntax**

```
arp resptime integer
no arp resptime
```

- `integer` — IP ARP entry response time out. (Range: 1-10 seconds)

**Default Configuration**
The default value is 1 second.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**
The following example defines a response time-out of 5 seconds.

```
console(config)#arp resptime 5
```
**arp retries**

Use the `arp retries` command in Global Configuration mode to configure the ARP count of maximum requests for retries. To return to the default value, use the `no` form of this command.

**Syntax**

arp retries integer  
no arp retries

- integer — The maximum number of requests for retries. (Range: 0-10)

**Default Configuration**

The default value is 4 retries.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example defines 6 as the maximum number of retries.

```
console(config)#arp retries 6
```

**arp timeout**

Use the `arp timeout` command in Global Configuration mode to configure the ARP entry age-out time. Use the `no` form of the command to set the age-out time to the default.

**Syntax**

arp timeout integer  
no arp timeout

- integer — The IP ARP entry age-out time. (Range: 15-21600 seconds)
Default Configuration
The default value is 1200 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example defines 900 seconds as the timeout.
console(config)#arp timeout 900

clear arp-cache
Use the clear arp-cache command to remove all ARP entries of type dynamic from the ARP cache.

Syntax
clear arp-cache [vrf vrf-name] [gateway]
  • vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, counters for the default (global) router instance is cleared.
  • gateway — Removes the dynamic entries of type gateway, as well.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
The VRF identified in the parameter must have been previously created or an error is returned.
Example
The following example clears all entries ARP of type dynamic, including gateway, from ARP cache.

console#clear arp-cache gateway

clear arp-cache management

Use the clear arp-cache management command to clear all entries that show as management arp entries in the show arp command.

Syntax
clear arp-cache management

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
In the example below, out-of-band management entries are shown, for example, those from the out-of-band interface.

console#show arp

Age Time (seconds)....................... 1200
Response Time (seconds)............... 1
Retries...................................... 4
Cache Size................................. 6144
Dynamic Renew Mode...................... Disable
Total Entry Count Current / Peak..... 0 / 0
Static Entry Count Configured / Active / Max.. 0 / 0 / 128

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Interface</th>
<th>Type</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.27.20.241</td>
<td>001A.A0FF.F662</td>
<td>Management</td>
<td>Dynamic</td>
<td>n/a</td>
</tr>
<tr>
<td>10.27.20.243</td>
<td>0019.B9D1.29A3</td>
<td>Management</td>
<td>Dynamic</td>
<td>n/a</td>
</tr>
</tbody>
</table>

console#clear arp-cache management
**ip local-proxy-arp**

Use the `ip local-proxy-arp` command in Interface Configuration mode to enable proxying of ARP requests. This allows the switch to respond to ARP requests within a subnet where routing is not enabled.

**Syntax**

```
ip local-proxy-arp
no ip local-proxy-arp
```

**Default Configuration**

Proxy arp is disabled by default.

**Command Mode**

Interface (VLAN) Configuration

**User Guidelines**

This command has no user guidelines.

**Example**

This example enables proxying of ARP requests on VLAN 10.

```
console(config-if-Gi1/0/1)#interface vlan 10
console(config-if-vlan10)#ip local-proxy-arp
```

**ip proxy-arp**

Use the `ip proxy-arp` command in Interface Configuration mode to enable proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request. Use the `no` form of the command to disable proxy ARP on a router interface.
**Syntax**

ip proxy-arp
no ip proxy-arp

**Default Configuration**

Enabled is the default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The `ip proxy-arp` command is not available in interface range mode.

**Example**

The following example enables proxy arp for VLAN 15.

```
(config)#interface vlan 15
console(config-if-vlan15)#ip proxy-arp
```

**show arp**

Use the `show arp` command to display all entries in the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the show ARP results.

**Syntax**

`show arp [vrf vrf-name] [brief]`

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- brief — Display ARP parameters.

**Default Configuration**

This command has no default configuration.
**Command Mode**

User Exec and Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

The show arp command will display static (user-configured) ARP entries regardless of whether they are reachable over an interface or not.

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example**

The following example shows `show arp` command output.

```
console#show arp
Static ARP entries are only active when the IP address is reachable on a local subnet

Age Time (seconds)......................... 1200
Response Time (seconds)..................... 1
Retries...................................... 4
Cache Size.................................. 6144
Dynamic Renew Mode......................... Disable
Total Entry Count Current / Peak........... 0 / 0
Static Entry Count Configured / Active / Max .. 1 / 0 / 128

IP Address MAC Address    Interface  Type   Age
---------- -------------- ---------  ------ -------
1.1.1.3    0000.0000.0022  n/a       Static n/a
```
Bidirectional Forwarding Detection Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

Bidirectional Forwarding Detection (BFD) verifies bidirectional connectivity between forwarding engines, which can be a single hop or multiple hops away. The protocol works over any underlying transmission mechanism and protocol layer with a wide range of detection times, especially in scenarios where fast failure detection is required in data plane level for multiple concurrent sessions.

Use the following commands to configure Bidirectional Forwarding Detection commands (BFD).

Commands in this Section

This section explains the following commands:

| feature bfd | ip ospf bfd |
| bfd echo | ipv6 ospf bfd |
| bfd interval | neighbor fall-over bfd |
| bfd slow-timer | show bfd neighbor |

**feature bfd**

Use this command to enable BFD on the router. Use the **no** form of the command to disable BFD and clear any dynamic state.

**Syntax**

```
feature bfd
no feature bfd
```

**Default Configuration**

BFD is not enabled by default.
**Command Mode**

Global Configuration

**User Guidelines**

BFD supports fast detection of forwarding failures on a routing interface. BFD provides an advantage for forwarding plane failure detection over that provided by the individual protocols, each having different hello protocol timers and detection periods.

The BFD feature provides notification to BGP or OSPF when an interface is detected to not be in a forwarding state. No other routing protocols are supported.

BFD is supported in the default VRF only.

BFD should be configured on routed interfaces only. BFD should not be configured on mirrored ports or on interfaces enabled for IEEE 802.1x.

BFD is supported across link aggregation groups, but does not detect individual LAG member link failure.

BFD does not operate on the out-of-band interface.

The `no feature bfd` command does not remove administrator-supplied configuration.

A BFD session is created per VLAN routing interface. On trunk ports, multiple BFD sessions may be established.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console# configure
console(config)# feature bfd
console(config)# exit
```

**bfd echo**

This command enables BFD echo mode on an interface. Use the `no` form of the command to disable BFD echo mode.
Syntax
bfd echo
no bfd echo

Default Configuration
BFD echo mode is not enabled by default.

Command Mode
Interface (VLAN) Configuration and Interface (VLAN) range mode.

User Guidelines
BFD echo mode enables fast sending and turnaround of BFD echo packets. Use the bfd slow-timer command to adjust the sending of BFD control plane packets when BFD echo mode is enabled.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console# configure
console(config)# interface vlan 10
console(config-if-vlan10)# bfd echo

bfd interval
This command configures BFD session parameters for a VLAN routing interface. It overwrites any BFD configuration present on the interface. Use the no form of the command to return the parameters to their default values.

Syntax
bfd interval transmit-interval min_rx min rx minimum-receive-interval multiplier
detection-time-multiplier
no bfd interval
• transmit-interval—Refers to the desired minimum transmit interval, which is the minimum interval the user wants to use while transmitting BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms with a change granularity of 100 ms and with a default value of 100 ms.

• minimum-receive-interval—Refers to the required minimum receive interval, which is the minimum interval at which the system can receive BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms with a granularity of 100 ms and with a default value of 100 ms.

• detection-time-multiplier—Specifies the number of BFD control packets which, if missed consecutively, will cause a session to be declared down. Its range is 3 to 50 with a default value of 3.

Default Configuration
The default transmit-interval is 100ms.
The default minimum-receive-interval is 100ms.
The default detection-time-multiplier is 3.

Command Mode
Interface (VLAN) mode.

User Guidelines
There are no user guidelines for this command.

Command History
Introduced in version 6.2.0.1 firmware.

Example
In this example, VLAN 100 is created, assigned an IP address to make it a routable interface, and the bfd interval is set to 100 ms, the minimum receive interface is 100 ms, and the multiplier is 5.

crash console#configure
console(config)#vlan 100
console(config-vlan100)#exit
console(config)#interface vlan 100
console(config-if-vlan100)#ip address 192.168.10.11 /24
console(config-if-vlan100)#bfd interval 100 min_rx 100 multiplier 5
console(config-if-vlan100)#exit
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport mode trunk

**bfd slow-timer**

This command configures the BFD periodic slow transmission interval for BFD Control packets. Use the no form of the command to return the slow transmission interval value to the default.

**Syntax**

```
bfd slow-timer receive-interval
no bfd slow-timer
```

- receive-interval—The slow transmission interval. Range 1000–30000 milliseconds.

**Default Configuration**

The default receive-interval is 2000 ms.

**Command Mode**

Global Configuration mode

**User Guidelines**

The argument receive-interval refers to the slow transmission interval for BFD Control packets. This timer is only used when the BFD echo function is enabled. When the BFD echo mode is enabled, the rate of BFD control packets is kept low as the echo function is used to detect forwarding failures.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console# configure
c内阁(config)# bfd slow-timer 1000
```
**ip ospf bfd**

Use the `ip ospf bfd` command to enable sending of BFD events to OSPF on a VLAN routing interface. Use the `no` form of the command to disable sending of BFD events.

**Syntax**

- `ip ospf bfd`
- `no ip ospf bfd`

**Default Configuration**

BFD is not enabled by default.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

BFD processing notifies OSPF of L3 connectivity issues with the peer. The interface must be a VLAN interface enabled for routing.

BFD must also be enabled in OSPF router configuration mode in order to BFD processing to occur.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example:

```
console#configure
cpu
console(config)#ip routing
console(config)#interface vlan 3
console(config-if-vlan3)#ip address 192.168.0.1/24
console(config-if-vlan3)#ip ospf area 0
console(config-if-vlan3)#ip ospf bfd
console(config-if-vlan3)#exit
console(config)#router ospf
console(config-router)#bfd
```
**ipv6 ospf bfd**

Use the `ipv6 ospf bfd` command to enable sending of BFD events to OSPF on a VLAN routing interface. Use the `no` form of the command to disable sending of BFD events.

**Syntax**

`ipv6 ospf bfd`
`no ipv6 ospf bfd`

**Default Configuration**

BFD is not enabled by default.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

BFD processing notifies OSPFv3 of level 3 connectivity issues with the peer. The interface must be a VLAN interfaced enabled for routing.

BFD must also be enabled in OSPFv3 router configuration mode for BFD processing to occur.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#configure
console(config)#ipv6 unicast-routing
console(config)#interface vlan 3
console(config-if-vlan3)#ipv6 address fe80::1214
console(config-if-vlan3)#ipv6 ospf area 0
console(config-if-vlan3)#ipv6 ospf bfd
console(config-if-vlan3)#exit
console(config)#ipv6 router ospf
console(config-router6)#bfd
```
**neighbor fall-over bfd**

This command enables BFD support for a BGP neighbor. Use the `no` form of the command to disable BFD for the specified BGP neighbor.

**Syntax**

```plaintext
neighbor { ipv4-address | ipv6-address [interface vlan vlan-id] } fall-over bfd
no neighbor { ipv4-address | ipv6-address [interface vlan vlan-id] } fall-over bfd interval
```

- `ipv4-address`—The IPv4 address of a configured neighbor reachable over a VLAN routing interface expressed in dotted quad notation.
- `ipv6-address`—The IPv6 address of a configured neighbor reachable over an IPv6 VLAN routing interface.
- `vlan-id`—If specified, the VLAN on which the IPv6 address is configured.

**Default Configuration**

No BFD neighbors are configured by default.

**Command Mode**

Router BGP Configuration mode

**User Guidelines**

There are no user guidelines for this command.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```plaintext
console(config)# router bgp
console(config-router)# neighbor 172.16.11.6 fall-over bfd
```

**show bfd neighbor**

This command displays the neighbors for which BFD has established adjacencies.
Syntax

show bfd neighbor [details] [ip-address]

- **details**—Display additional information regarding each BFD neighbor, including sent and received message counts.
- **ip-address**—The IPv4 or IPv6 address of a BFD neighbor. Limits the output to the specific neighbor.

Default Configuration

There is no default configuration for this command.

Command Mode

User mode, Privileged Exec mode, Global Configuration mode, all show modes

User Guidelines

The local address displayed in the output is the IP address of the interface through which the neighbor is connected.

Update is displayed in the format dd hh:mm:ss where:

- **dd** is days
- **hh** is hours
- **mm** is minutes
- **ss** is seconds

The operational intervals are the intervals used as a result of negotiation with the BFD link partner.

The following information is displayed.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our IP address</td>
<td>The current IP address.</td>
</tr>
<tr>
<td>Neighbor IP address</td>
<td>The IP address of the active BFD neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>The current state, either Up or Down.</td>
</tr>
<tr>
<td>Interface</td>
<td>The current interface.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time the interface has been up.</td>
</tr>
</tbody>
</table>
**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Protocol</td>
<td>The protocol from which the BFD session was initiated and that is registered to receive events from BFD. (for example, BGP).</td>
</tr>
<tr>
<td>Local Diag</td>
<td>The diagnostic state specifying the reason for the most recent change in the local session state.</td>
</tr>
<tr>
<td>Demand mode</td>
<td>Indicates if the system wishes to use Demand mode.</td>
</tr>
<tr>
<td>Minimum transmit interval</td>
<td>The minimum interval to use when transmitting BFD control packets.</td>
</tr>
<tr>
<td>Actual TX Interval</td>
<td>The transmitting interval being used for control packets.</td>
</tr>
<tr>
<td>Actual TX Echo interval</td>
<td>The transmitting interval being used for echo packets.</td>
</tr>
<tr>
<td>Minimum receive interval</td>
<td>The minimum interval at which the system can receive BFD control packets.</td>
</tr>
<tr>
<td>Detection interval multiplier</td>
<td>The number of BFD control packets that must be missed in a row to declare a session down.</td>
</tr>
<tr>
<td>My discriminator</td>
<td>Unique Session Identifier for Local BFD Session.</td>
</tr>
<tr>
<td>Your discriminator</td>
<td>Unique Session Identifier for Remote BFD Session.</td>
</tr>
<tr>
<td>Tx Count</td>
<td>The number of transmitted BFD packets.</td>
</tr>
<tr>
<td>Rx Count</td>
<td>The number of received BFD packets.</td>
</tr>
<tr>
<td>Drop Count</td>
<td>The number of dropped packets.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console# show bfd neighbors

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Neighbor</th>
<th>Uptime</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.1</td>
<td>172.16.10.20</td>
<td>02:18:49</td>
<td>Up</td>
<td>VLAN10</td>
</tr>
<tr>
<td>10.1.10.1</td>
<td>10.1.10.20</td>
<td>01:15:25</td>
<td>Up</td>
<td>Gi1/0/5</td>
</tr>
<tr>
<td>fdf8:f53b::53</td>
<td>fdf8:f53b::58</td>
<td>00:38:11</td>
<td>Up</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

console# show bfd neighbors details
```
Local IP address......................... 2.1.1.1
Neighbor IP address...................... 2.1.1.2
State.................................... Up
Interface.................................. VLAN 10
Uptime................................... 0:00:01:54
Registered Protocol...................... BGP
Local Diag................................ 0
Demand mode.............................. FALSE
Minimum transmit interval............... 100 ms
Minimum receive interval................ 100 ms
Operational transmit interval........... 100 ms
Operational transmit echo interval...... 0 ms
Detection interval multiplier.......... 3
Local discriminator..................... 1
Remote discriminator.................... 1
Tx Count.................................. 105
Rx Count.................................. 107
Drop Count............................... 0
Border Gateway Protocol Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

This section describes the commands you use to view and configure Border Gateway Protocol (BGP), which is an exterior gateway routing protocol that you use to route traffic between autonomous systems. The BGP CLI commands are available in the N3000/N3100/N4000 Series switches. On the N3000 Series switches, the BGP specific firmware must be loaded (e.g., N3000_BGPvA.B.C.D.stk.

**CAUTION:** The commands in this section are in one of three functional groups.

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands reset part of the protocol state.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp</td>
<td>maximum-paths (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td>address-family</td>
<td>maximum-paths ibgp (BGP Router Configuration)</td>
</tr>
<tr>
<td>address-family ipv4 vrf</td>
<td>maximum-paths ibgp (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td>address-family ipv6</td>
<td>neighbor activate</td>
</tr>
<tr>
<td>address-family vpnv4 unicast</td>
<td>neighbor advertisement-interval (BGP Router Configuration)</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>aggregate-address</code></td>
<td>neighbor advertisement-interval (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td><code>bgp aggregate-different-meds</code> (BGP Router Configuration)</td>
<td>neighbor allowas-in</td>
</tr>
<tr>
<td><code>bgp aggregate-different-meds</code> (IPv6 Address Family Configuration)</td>
<td>neighbor connect-retry-interval</td>
</tr>
<tr>
<td><code>bgp always-compare-med</code></td>
<td>neighbor default-originate (BGP Router Configuration)</td>
</tr>
<tr>
<td><code>bgp client-to-client reflection</code> (BGP Router Configuration)</td>
<td>neighbor default-originate (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td><code>bgp client-to-client reflection</code> (IPv6 Address Family Configuration)</td>
<td>neighbor description</td>
</tr>
<tr>
<td><code>bgp cluster-id</code></td>
<td>neighbor ebgp-multihop</td>
</tr>
<tr>
<td><code>bgp default local-preference</code></td>
<td>neighbor filter-list (BGP Router Configuration)</td>
</tr>
<tr>
<td><code>bgp fast-external-fallover</code></td>
<td>neighbor filter-list (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td><code>bgp fast-internal-fallover</code></td>
<td>neighbor inherit peer</td>
</tr>
<tr>
<td><code>bgp listen</code></td>
<td>neighbor local-as</td>
</tr>
<tr>
<td><code>bgp log-neighbor-changes</code></td>
<td>neighbor maximum-prefix (BGP Router Configuration)</td>
</tr>
<tr>
<td><code>bgp maxas-limit</code></td>
<td>neighbor maximum-prefix (IPv6 Address Family Configuration)</td>
</tr>
<tr>
<td><code>bgp router-id</code></td>
<td>neighbor next-hop-self (BGP Router Configuration)</td>
</tr>
<tr>
<td>Command</td>
<td>Command</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>neighbor next-hop-self</td>
</tr>
<tr>
<td>clear ip bgp counters</td>
<td>neighbor password</td>
</tr>
<tr>
<td>default-information originate (BGP Router</td>
<td>neighbor prefix-list (BGP Router Configuration)</td>
</tr>
<tr>
<td>Configuration)</td>
<td>default-information originate (IPv6 Address</td>
</tr>
<tr>
<td></td>
<td>Address Family Configuration)</td>
</tr>
<tr>
<td>default metric (BGP Router Configuration)</td>
<td>neighbor prefix-list (IPv6 Address Family</td>
</tr>
<tr>
<td></td>
<td>Configuration)</td>
</tr>
<tr>
<td>default metric (IPv6 Address Family</td>
<td>neighbor remote-as</td>
</tr>
<tr>
<td>Configuration)</td>
<td>neighbor remove-private-as</td>
</tr>
<tr>
<td>distance</td>
<td>neighbor rfc5549-support</td>
</tr>
<tr>
<td>distance bgp (BGP Router Configuration)</td>
<td>neighbor route-map (BGP Router Configuration)</td>
</tr>
<tr>
<td>distance bgp (IPv6 Address Family Configuration)</td>
<td>neighbor route-map (IPv6 Address Family</td>
</tr>
<tr>
<td></td>
<td>Configuration)</td>
</tr>
<tr>
<td>distribute-list prefix in</td>
<td>neighbor route-reflector-client (BGP Router</td>
</tr>
<tr>
<td></td>
<td>Configuration)</td>
</tr>
<tr>
<td>distribute-list prefix out (BGP Router</td>
<td>neighbor route-reflector-client (IPv6 Address</td>
</tr>
<tr>
<td>Configuration)</td>
<td>Address Family Configuration)</td>
</tr>
<tr>
<td>distribute-list prefix out (IPv6 Address</td>
<td>neighbor send-community</td>
</tr>
<tr>
<td>Configuration)</td>
<td>(BGP Router Configuration)</td>
</tr>
<tr>
<td>enable</td>
<td>neighbor send-community</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>neighbor shutdown</td>
</tr>
</tbody>
</table>
router bgp

Use the `router bgp` command to enable BGP and identify the autonomous system (AS) number for the router. Only a single instance of BGP can be run and the router can only belong to a single AS.

**Syntax**

```
router bgp as-number
no router bgp as-number

• as-number—The router’s autonomous system number is asplain format. Dell EMC Networking BGP supports two byte AS numbers, in the range of 0-65535.
```

**Default Configuration**

By default, BGP is inactive.

**Command Mode**

Global Configuration mode

**User Guidelines**

The `no router bgp` command disables BGP and all BGP configurations revert to default values. Alternatively, the administrator can use the `no enable` command in BGP router configuration mode to disable BGP globally without clearing the BGP configuration.
ASNs 0, 56320–64511, and 65535 are reserved and cannot be used.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

The following example creates a BGP routing instances and enables BGP routing for AS 4324.

```
console(config)#router bgp 4324
```

**address-family**

Use the `address-family` command in peer template configuration mode to configure policy parameters within a peer template to be applied to a specific address family. To delete all policy commands for an address family in a peer template, use the `no` form of this command.

**Syntax**

```
address-family { ipv4 | ipv6 }
no address-family { ipv4 | ipv6 }
```

- `ipv4`—Configure policy parameters to be applied to IPv4 routes.
- `ipv6`—Configure policy parameters to be applied to IPv6 routes.

**Default Configuration**

No peer templates are configured by default.

**Command Mode**

Peer Template Configuration mode

**User Guidelines**

This command enters address family configuration mode within the peer template. Policy commands configured within this mode apply to the address family. The following commands can be added to a peer template in address family configuration mode:

- `activate`
• `advertisement-interval` seconds
• `default-originate`
• `filter-list` `as-path-list-number` `{in | out}`
• `maximum-prefix` `{ maximum | unlimited } [threshold]`
• `next-hop-self`
• `prefix-list` `prefix-list-name` `{ in | out }`
• `remove-private-as`
• `route-reflector-client`
• `route-map` `map-name` `{ in | out }
• `send-community`

The `activate` command is only available in `address-family ipv6` mode.

If an IPv6 peer inherits a template that specifies `address family ipv4` parameters, those parameters are ignored.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

In this example, the peer template AGGR sets the keepalive timer to 3 seconds and the hold timer to 9 seconds, allows communities to be sent for both IPv4 and IPv6 routes, and configures different inbound and outbound route maps for IPv4 and IPv6. Two neighbors, 172.20.1.2 and 172.20.2.2, inherit these parameters from the template.

```
cp(config)# router bgp 65000
cp(config-router)# neighbor 172.20.1.2 remote-as 65001
cp(config-router)# neighbor 172.20.2.2 remote-as 65001
cp(config-router)# template peer AGGR
cp(config-rtr-tmplt)# timers 3 9
cp(config-rtr-tmplt)# address-family ipv4
   cp(config-rtr-tmplt-af)# send-community
   cp(config-rtr-tmplt-af)# route-map RM4-IN in
   cp(config-rtr-tmplt-af)# route-map RM4-OUT out
   cp(config-rtr-tmplt-af)# exit
   cp(config-rtr-tmplt)# address-family ipv6
   cp(config-rtr-tmplt-af)# send-community
   cp(config-rtr-tmplt-af)# route-map RM6-IN in
   cp(config-rtr-tmplt-af)# route-map RM6-OUT out
   cp(config-rtr-tmplt-af)# exit
```
Layer 3 Routing Commands

address-family ipv4 vrf

Use the address-family ipv4 vrf command to enter IPv4 VRF configuration mode for a particular VRF instance to configure the BGP VRF parameters. Use the no form of this command to delete the IPv4 VRF configuration.

Syntax
address-family ipv4 vrf vrf-name
no address-family ipv4 vrf vrf-name
  • vrf-name — The VRF instance name.

Default Configuration
There is no default configuration.

Command Mode
BGP Router Configuration mode

User Guidelines
Commands entered in this mode enable peering with BGP neighbors in this VRF instance. All the neighbor specific commands are given in this mode as well.
VRF configuration is disabled by default.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console(config-router)# address-family ipv4 vrf Red
address-family ipv6

Use the **address-family ipv6** command to enter IPv6 family configuration mode to specify IPv6 configuration parameters. Use the **no** form of the command to delete all IPv6 configuration.

**Syntax**

address-family ipv6

no address-family ipv6

**Default Configuration**

By default, the exchange of IPv6 routes is disabled.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

The **address-family ipv6** command moves the CLI to IPv6 address family configuration mode. Commands entered in this mode can be used to enable exchange of IPv6 routes over IPv6 or IPv4 peering sessions, specify IPv6 prefixes to be originated, and configure inbound and outbound policies to be applied to IPv6 routes. The **no** version of this command clears all IPv6 address family configuration.

ASNs 0, 56320–64511, and 65535 are reserved cannot be used.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)# address-family ipv6
```

address-family vpnv4 unicast

Use the **address-family vpnv4 unicast** command to configure a BGP routing session to advertise VPN IPv4 prefixes.

Use the **no** form of this command to delete the VPN IPv4 configuration.
Syntax
address-family vpn4 unicast
no address-family vpn4 unicast

Default Configuration
VPN-IPv4 address family mode is not configured by default.

Command Mode
Router BGP Configuration mode

User Guidelines
When an iBGP neighbor is configured in this mode, each VPN-IPv4 prefix is made globally unique by the addition of an 8-byte route distinguisher (RD). Only unicast prefixes are advertised to the iBGP neighbor. To exit from VPN-IPv4 address family mode, use the exit command.

This command enters VPN-IPv4 address family configuration mode. All neighbor commands available in IPv4 Address Family configuration mode are applicable to this mode as well.

Two additional options to the neighbor command are available in VPN-IPv4 address family configuration mode. See the bold keywords in the commands below for the additions:
- neighbor ip-address activate
- neighbor ip-address send-community extended

Command History
Introduced in version 6.3.0.1 firmware.

Example
The following example shows how to enter the VPN-IPv4 address family mode and to distribute VPN4-IPv4 addresses to a neighbor with the extended community attribute:

```
console(config)# router bgp 10
console(config-router)# neighbor 1.1.1.1 remote-as 5000
console(config-router)# address-family vpnv4 unicast
console(config-router-af)# neighbor 1.1.1.1 activate
```
aggregate-address

Use the aggregate-address command to configure a summary address for BGP.

Syntax

```shell
aggregate-address { ipv4-prefix mask | ipv6-prefix/prefix-length } [as-set] [summary-only]
no aggregate-address { ipv4-prefix mask | ipv6-prefix/prefix-length } [as-set] [summary-only]
```

- `ipv4-prefix mask`—A summary prefix and mask in dotted-quad notation. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid IPv4 unicast destination prefix.

- `ipv6-prefix`—An IPv6 network prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons. Counters are cleared only for the matching prefixes.

- `prefix-length`—The length of the IPv6 prefix given as part of the ipv6-prefix. This is required if a prefix is specified. A decimal value in the range 0 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash must precede the decimal value in /length format.

- `as-set`—If the as-set option is configured, the aggregate is advertised with a non-empty AS_PATH. (Normally, the aggregate is advertised with an empty AS path and the ATOMIC_AGGREGATE attribute.) If the AS_PATH of all contained routes is the same, the AS_PATH of the aggregate is the AS_PATH of the contained routes. Otherwise, if the contained routes have different AS_PATHs, the AS_PATH attribute includes an AS_SET with each of the AS numbers listed in the AS PATHs of the aggregated routes. If the as-set option is not configured, the aggregate is advertised with an empty AS_PATH.
• summary-only — When specified, the more-specific routes within the aggregate address are not advertised to neighbors.

**Default Configuration**

No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

**Command Mode**

- BGP Router Configuration mode
- IPv6 Address Family Configuration mode

**User Guidelines**

To be considered a match for an aggregate address, a prefix must be more specific (i.e., have a longer prefix length) than the aggregate address. A prefix whose prefix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix but not a more specific route match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```console
console(config-router)#aggregate-address 10.27.21.0 255.255.255.0
```

**bgp aggregate-different-meds (BGP Router Configuration)**

Use the `bgp aggregate-different-meds` command to control the aggregation of routes with different multi-exit discriminator (MED) attributes. By default, BGP only aggregates routes that have the same MED value.
Syntax
bgp aggregate-different-meds
no bgp aggregate-different-meds

Default Configuration
By default, all the routes aggregated by a given aggregate address must have the same MED value.

Command Mode
BGP Router Configuration mode

User Guidelines
When this command is used, the path for an active aggregate address is advertised without an MED attribute and the MED attribute is not considered in aggregating routes. When this command is not used, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route and any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered part of the aggregate and continue to be advertised as individual routes.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#bgp aggregate-different-meds

bgp aggregate-different-meds (IPv6 Address Family Configuration)
Use the bgp aggregate-different-meds command to allow IPv6 routes with different MEDs to be aggregated.

Syntax
bgp aggregate-different-meds
no bgp aggregate-different-meds

**Default Configuration**
By default, all the routes aggregated by a given aggregate address must have the same MED value.

**Command Mode**
IPv6 Address Family Configuration mode

**User Guidelines**
When this command is used, the path for an active aggregate address is advertised without an MED attribute and the MED attribute is not considered in aggregating routes. When this command is not used, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route and any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered part of the aggregate and continue to be advertised as individual routes.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config-router-af)#bgp aggregate-different-meds
```

**bgp always-compare-med**
Use this command to compare MED values during the decision process in paths received from different autonomous systems. To revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS, use the no form of this command.

**Syntax**
```
bgp always-compare-med
no bgp always-compare-med
```
Default Configuration
By default, all routes aggregated by a given aggregate address must have the same MED value.

Command Mode
- BGP Router Configuration mode
- IPv6 Address Family Configuration mode

User Guidelines
The MED is a 32-bit integer, commonly set by an external peer to indicate the internal distance to a destination. The decision process compares MED values to prefer paths that have a shorter internal distance. Since different autonomous systems may use different internal distance metrics or have different policies for setting the MED, the decision process normally does not compare MED values in paths received from peers in different autonomous systems. This command allows you to force BGP to compare MEDs regardless of if paths are received from a common AS.

Command History
Introduced in version 6.2.0.1 firmware.

Example
```
console(config-router)#bgp always-compare-med
```

bgp client-to-client reflection (BGP Router Configuration)
Use the bgp client-to-client reflection command to enable client-to-client reflection. By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector’s clients have a full iBGP mesh, the route reflector does not reflect to the clients.

Syntax
```
bgp client-to-client reflection
no bgp client-to-client reflection
```
**Default Configuration**

Client-to-client reflection is enabled by default when a router is configured as a route reflector.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be influenced by the IGP metric of the route to reach the BGP next hop. Since a client’s IGP distance to a given next hop may differ from route reflector’s IGP distance, a route reflector may not re-advertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When clients are fully meshed, there is no need for the cluster’s route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

In BGP Router Configuration mode, this command only affects advertisement of IPv4 routes. The same command is available in Address-Family IPv6 Configuration mode for IPv6 routes.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```console
console(config-router)#bgp client-to-client reflection
```

**bgp client-to-client reflection (IPv6 Address Family Configuration)**

Use the `bgp client-to-client reflection` command to enable client-to-client reflection. By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector’s clients have a full iBGP mesh, the route reflector does not reflect to the clients.
**Syntax**

bgp client-to-client reflection
no bgp client-to-client reflection

**Default Configuration**

Client-to-client reflection is enabled by default when a router is configured as a route reflector.

**Command Mode**

IPv6 Address Family Configuration mode

**User Guidelines**

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be influenced by the IGP metric of the route to reach the BGP next hop. Since a client’s IGP distance to a given next hop may differ from route reflector’s IGP distance, a route reflector may not re-advertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When clients are fully meshed, there is no need for the cluster’s route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

The same command is available in BGP Router Configuration mode for IPv4 routes.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

console(config-router-af)#bgp client-to-client reflection

**bgp cluster-id**

Use the bgp cluster-id command to specify the cluster ID of a route reflector. To revert the cluster ID to its default, use the no form of this command.
Syntax

bgp cluster-id cluster-id
no bgp cluster-id

- cluster-id—A non-zero 32-bit identifier that uniquely identifies a cluster of route reflectors and their clients. The cluster ID may be entered in dotted notation like an IPv4 address or as an integer.

Default Configuration

A route reflector whose cluster ID has not been configured uses its BGP router ID (configured with bgp router-id) as the cluster ID.

Command Mode

BGP Router Configuration mode

User Guidelines

A route reflector and its clients form a cluster. Since a cluster with a single route reflector has a single point of failure, a cluster may be configured with multiple route reflectors. To avoid sending multiple copies of a route to a client, each route reflector in a cluster should be configured with the same cluster ID. Route reflectors with the same cluster ID must have the same set of clients; otherwise, some routes may not be reflected to some clients. The same cluster ID is used for both IPv4 and IPv6 route reflection.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-router)#bgp cluster-id 1

bgp default local-preference

Use the bgp default local-preference command to enable the network operator to specify the default local preference. Local preference is an attribute sent to internal peers to indicate the degree of preference for a route. A route with a numerically higher local value is preferred over a route with a numerically lower value.
Syntax

bgp default local-preference number
no bgp default local-preference

- number—The value to use as the local preference for routes advertised to internal peers. The range is 0 to 4,294,967,295.

Default Configuration

If no other value is configured, BGP advertises a local preference of 100 in UPDATE messages to internal peers.

Command Mode

BGP Router Configuration mode

User Guidelines

BGP assigns the default local preference to each path received from an external peer. (BGP retains the LOCAL_PREF on paths received from internal peers.) BGP also assigns the default local preference to locally-originated paths. If you change the default local preference, the local preference on paths previously received is not changed; it is only applied to paths received after the change. To apply the new local preference to paths previously received, use clear ip bgp to force a soft inbound reset.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-router)#bgp default local-preference 1

bgp fast-external-fallover

Use this command to configure BGP to immediately reset the adjacency with an external peer if the routing interface to the peer goes down.

Syntax

bgp fast-external-fallover
no bgp fast-external-fallover

**Default Configuration**
Fast external fallover is enabled by default.

**Command Mode**
BGP Router Configuration mode

**User Guidelines**
When BGP gets a routing interface down event, BGP drops the adjacency with all external peers whose IPv4 address is in one of the subnets on the failed interface. This behavior can be overridden for specific interfaces using ip bgp fast-external-fallover.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
console(config-router)# bgp fast-external-fallover

```
bgp fast-internal-fallover
```

Use the **bgp fast-internal-fallover** command to configure BGP to immediately reset the adjacency with an internal peer when there is a loss of reachability to an internal peer.

**Syntax**
bgp fast-internal-fallover
no bgp fast-internal-fallover

**Default Configuration**
By default, fast internal fallover is enabled.

**Command Mode**
BGP Router Configuration mode
User Guidelines
BGP tracks the reachability of each internal peer’s IP address. If a peer becomes unreachable (that is, the RIB no longer has a non-default route to the peer’s IP address), BGP drops the adjacency.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)# bgp fast-internal-fallover

bgp listen
Use the bgp listen command to create an IPv4 listen range and associates it with the specified peer template. The bgp listen command also activates the IPv4 or IPv6 BGP dynamic neighbors feature. Use the no form of the command to remove an IPv4 or IPv6 listen range.

Syntax
bgp listen { limit max-number | range network/length [ inherit peer peer-template-name ] }
no bgp listen { limit | range network/length [ inherit peer peer-template-name ] }

- **limit max-number** — Sets a maximum limit number of IPv4 BGP dynamic subnet range neighbors. The number is from 1 to 100. Default is 20.
- **range network/length** — Specifies a listen subnet range that is to be created. The IP prefix representing a subnet is specified by network, and length is the subnet mask in bits. The network argument can be valid IPv4 prefix (BGP Router Configuration mode or IPv4 Address Family Configuration mode) or an IPv6 prefix (IPv6 Address Family Configuration mode).
- **inherit peer peer-template-name** — (Optional) Specifies a BGP peer template name that is to be associated with the specified listen subnet range and inherited with dynamically created neighbors.
**Default Configuration**

No subnets are associated with a BGP listen subnet range, and the BGP dynamic neighbor feature is not activated.

**Command Mode**

BGP Router Configuration mode, IPv4 Address Family Configuration mode, IPv6 Address Family Configuration mode

**User Guidelines**

This command can be used to configure IPv4 BGP neighbors (BGP Router Configuration mode) as well as IPv6 BGP neighbors (IPv6 Address Family Configuration mode).

Use the `limit` keyword and max-number argument to define the global maximum number of IPv4 BGP dynamic neighbors that can be created.

BGP dynamic neighbors are configured using a range of IP addresses. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group, and a TCP session is initiated by the neighbor for an IP address in the subnet range, a new BGP neighbor is dynamically configured on the local switch. Dynamically created neighbors are not displayed in the running-config.

It is acceptable that the template peer name is not specified. In this case, all dynamic neighbors are created with the default parameters. The template peer name can be assigned/changed for a listen range at any time.

The limit on the total number of both IPv4 and IPv6 listen range groups is 10.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example shows how to create an IPv4 listen range with a template to be inherited with dynamically created BGP neighbors:

```
console#configure
console(config)# router bgp 100
console(config-router)# bgp listen limit 10
console(config-router)# bgp listen range 10.12.0.0/16
console(config-router)# bgp listen range 10.27.0.0/16 inherit peer ABC
```
**bgp log-neighbor-changes**

Use the `bgp log-neighbor-changes` command to enable logging of adjacency state changes.

**Syntax**

`bgp log-neighbor-changes`

`no bgp log-neighbor-changes`

**Default Configuration**

Neighbor state changes are not logged by default.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

Both backward and forward adjacency state changes are logged. Forward state changes, except for transitions to the Established state, are logged at the Informational severity level. Backward state changes and forward changes to Established are logged at the Notice severity level.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)# bgp log-neighbor-changes
```

**bgp maxas-limit**

Use this command to specify a limit on the length of AS Paths that BGP accepts from its neighbors. To revert the limit to its default, use the `no` form of this command.

**Syntax**

`bgp maxas-limit limit`

`no bgp maxas-limit`
• limit—The maximum length of an AS Path that BGP accepts from its
neighbors. The length is the number of autonomous systems listed in the
path. The limit may be set to any value from 1 to 100.

Default Configuration
BGP accepts AS paths with up to 75 AS numbers

Command Mode
BGP Router Configuration mode

User Guidelines
If BGP receives a path whose AS PATH attribute is longer than the configured
limit, BGP sends a NOTIFICATION and resets the adjacency.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#bgp maxas-limit 1

bgp router-id
Use the bgp router-id command to set the BGP router ID.

Syntax
bgp router-id router-id
no bgp router-id

• router-id—An IPv4 address in dotted quad notation. This is the address for
BGP to use as it’s router ID.

Default Configuration
There is no default BGP router ID. The system does not select a router ID
automatically. One must be configured manually.
**Command Mode**
BGP Router Configuration mode

**User Guidelines**
The BGP router ID must be a valid IPv4 unicast address, but is not required to be an address assigned to the router. The router ID is specified in the dotted notation of an IPv4 address. Changing the router ID disables and re-enables BGP, causing all adjacencies to be re-established.

BGP is enabled by default once the administrator has specified the local AS number with the `router bgp` command and configured a router ID with the `bgp router-id` command.

BGP is not operable until a BGP router ID has been assigned. The BGP administrative state (as set by the enable command) has no operational effect until a router id is assigned to the BGP router.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config-router)#bgp router-id 10.27.21.142
clear ip bgp
```

**clear ip bgp**
Use the `clear ip bgp` command to reset peering sessions with all of a subnet of BGP peers. The command arguments specify which peering sessions are reset and the type of reset performed.

**Syntax**
```
clear ip bgp [vrf vrf-name]{{ | as-number | ipv4-address | ipv6-address [interface interface-id ] {listen range network/length}} [soft [in | out]]
```
- vrf-name—This optional parameter identifies the VRF for which to reset peering sessions. If not given, the default sessions are reset.
- *—Reset adjacency with every BGP peer.
- as-number—Only reset adjacencies with BGP peers in the given autonomous system.
• **ipv4-address**—Only reset the adjacency with a single specified peer with a
given IPv4 peer address.

• **ipv6-address [ interface interface-id ]**—Only reset the adjacency with a
single specified peer with a given IPv6 peer address. If the interface-id is
given, only reset the adjacency on the specified interface. The interface id
must be a routing interface (a routed VLAN identifier). An adjacency that
is formed with the auto-detect feature cannot be reset with the command.

• **listen range** – Reset all adjacencies that are included in the listen subnet
range.

• **soft**—BGP resends all updates to the neighbors and reprocesses updates
from the neighbors.

• **in | out**—If the in keyword is given, updates from the neighbor are
reprocessed. If the out keyword is given, updates are resent to the neighbor.
If neither keyword is given, updates are reprocessed in both directions.

**Default Configuration**

There is no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

Soft inbound reset causes BGP to send a Route Refresh request to each
neighbor being reset. If a neighbor does not support the Route Refresh
capability, the updated policy is applied to routes previously received from the
neighbor.

When a change is made to an outbound policy, BGP schedules an outbound
soft reset to update neighbors according to the new policy.

This command applies to routes for all address families.

When **clear ip bgp** is issued for any peers, any pending policy configuration
changes are applied, for all global policy and for all peers.

**Command History**

Introduced in version 6.2.0.1 firmware. Updated in version 6.3.0.1 firmware.
clear ip bgp counters

Use the clear ip bgp counters resets all BGP counters to 0. These counters include send and receive packet and prefix counters for all neighbors.

Syntax

clear ip bgp [vrf vrf-name] counters

- vrf-name—This optional parameter identifies the VRF for which to clear counters. If not given, the default VRF counters are cleared.

Default Configuration

There is no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

There are no user guidelines.

Command History

Introduced in version 6.3.0.1 firmware.

default-information originate (BGP Router Configuration)

Use the default-information originate command to enable BGP to originate a default route.

Syntax

default-information originate [ always ]
no default-information originate Default Configuration

- always—Allows BGP to originate a default route even if the common routing table has no default route.

**Default Configuration**

By default BGP does not originate a default route. If a default route is redistributed into BGP, BGP does not advertise the default route unless the `default-information originate` command has been given. The `always` option is disabled by default.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

Origination of the default route is not subject to a prefix filter configured with the `distribute-list out` command.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#default-information originate
```

**default-information originate (IPv6 Address Family Configuration)**

Use this command in IPv6 Address Family Config mode to allow BGP to originate an IPv6 default route.

**Syntax**

default-information originate [ always ]

no default-information originate Default Configuration

- always—Allows BGP to originate a default route even if the common routing table has no default route.
Default Configuration
By default BGP does not originate a default route. If a default route is redistributed into BGP, BGP does not advertise the default route unless the default-information originate command has been given. The always option is disabled by default.

Command Mode
IPv6 Address Family Configuration mode

User Guidelines
Origination of the default route is not subject to a prefix filter configured with the distribute-list out command.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router-af)#default-information originate

default metric (BGP Router Configuration)
This command sets the value of the Multi Exit Discriminator (MED) attribute on routes redistributed into BGP when no metric has been specified in the redistribute command.

Syntax
default-metric value
no default-metric
  • value—The value to as the MED. The range is 1 to 4,294,967,295.

Default Configuration
By default, no default metric is set and no MED is included in redistributed routes.
**Command Mode**
BGP Router Configuration mode

**User Guidelines**
There are no user guidelines.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config-router)#default-metric 1
```

**default metric (IPv6 Address Family Configuration)**
This command sets the metric of redistributed IPv6 routes when a metric is not configured in the redistribute command.

**Syntax**
```
default-metric value
no default-metric
```
- **value**—The value to as the MED. The range is 1 to 4,294,967,295.

**Default Configuration**
By default, no default metric is set and no MED is included in redistributed routes.

**Command Mode**
IPv6 Address Family Configuration mode

**User Guidelines**
There are no user guidelines.
Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router-af)#default-metric 1

distance
Use this command to set the preference (also known as administrative distance) of BGP routes to specific destinations.

Syntax
distance distance [ prefix wildcard-mask [prefix-list] ]
no distance distance [ prefix wildcard-mask [prefix-list] ]

- distance—The preference value for matching routes. The range is 1 to 255.
- prefix wildcard-mask—Routes learned from BGP peers whose address falls within this prefix are assigned the configured distance value. The wildcard-mask is an inverted network mask whose 1 bits indicate the don’t care portion of the prefix.
- prefix-list—A prefix list can optionally be specified to limit the distance value to a specific set of destination prefixes learned from matching neighbors.

Default Configuration
BGP assigns preference values according to the distance bgp command, unless overridden for specific neighbors or prefixes by this command.

Command Mode
BGP Router Configuration mode

User Guidelines
You may enter up to 128 instances of this command. Two instances of this command may not have the same prefix and wildcard mask. If a distance command is configured that matches an existing distance command’s prefix and wildcard mask, the new command replaces the existing command. There
can be overlap between the prefix and mask configured for different commands. When there is overlap, the command whose prefix and wildcard mask are the longest match for a neighbor’s address is applied to routes from that neighbor.

An ECMP route’s distance is determined by applying distance commands to the neighbor that provided the best path.

The distance command is not applied to existing routes. To apply configuration changes to the distance command itself or the prefix list to which a distance command applies, you must force a hard reset of affected neighbors.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

To set the preference value of the BGP route to 100.0.0.0/8 from neighbor 10.1.1.1, use the following distance command:

```
(R1) (Config)# ip prefix-list pfx-list1 permit 100.0.0.0/8
(R1) (Config)# router bgp 1
(R1) (Config-router)# distance 25 10.1.1.1 0.0.0.0 pfx-list1
```

To set the preference value to 12 for all BGP routes from neighbor 10.1.1.1, use the following distance command:

```
(R1) (Config-router)# distance 12 10.1.1.1 0.0.0.0
```

To set the preference value of all routes within 100.0.0.0/8 from any neighbor, use the following distance command:

```
(R1) (Config)# ip prefix-list pfx-list2 permit 100.0.0.0/8 ge 8
(R1) (Config)# router bgp 1
(R1) (Config-router)#distance 25 0.0.0.0 255.255.255.255 pfx-list2
```

**distance bgp (BGP Router Configuration)**

Use this command to set the preference (also known as administrative distance) of BGP routes.

**Syntax**

distance bgp external-distance internal-distance local-distance

no distance bgp
• external-distance—The preference value for routes learned from external peers. The range is 1 to 255.
• internal-distance—The preference value for routes learned from internal peers. The range is 1 to 255.
• local-distance—The preference value for locally-originated routes. The range is 1 to 255.

**Default Configuration**
- external-distance—20
- internal-distance—200
- local-distance—200

**Command Mode**
BGP Router Configuration mode

**User Guidelines**
Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
console(config-router)#distance bgp 20 200 200

**distance bgp (IPv6 Address Family Configuration)**
Use this command to set the preference (also known as administrative distance) of BGP routes.
**Syntax**

distance bgp external-distance internal-distance local-distance

no distance bgp

- external-distance—The preference value for routes learned from external peers. The range is 1 to 255.
- internal-distance—The preference value for routes learned from internal peers. The range is 1 to 255.
- local-distance—The preference value for locally-originated routes. The range is 1 to 255.

**Default Configuration**

- external-distance—20
- internal-distance—200
- local-distance—200

**Command Mode**

IPv6 Address Family Configuration mode

**User Guidelines**

Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

console(config-router-af)#distance bgp 20 200 200
**distribute-list prefix in**

Use this command to configure a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.

**Syntax**

distribute-list prefix list-name in

no distribute-list prefix list-name in

- list-name—A prefix list used to filter routes received from all peers based on destination prefix.

**Default Configuration**

No distribute lists are defined by default.

**Command Mode**

- BGP Router Configuration mode
- IPv6 Address Family Configuration mode

**User Guidelines**

The distribute list is applied to all routes received from all neighbors. Only routes permitted by the prefix list are accepted. If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
croutle(config-router)#distribute-list prefix 255 in
```

**distribute-list prefix out (BGP Router Configuration)**

Use this command to configure a filter that restricts the advertisement of routes based on destination prefix.
Syntax

distribute-list prefix list-name out [ protocol | connected | static ]

no distribute-list prefix list-name out [ protocol | connected | static ]

- prefix list-name—A prefix list used to filter routes advertised to neighbors.
- protocol|connected|static—(Optional) When a route source is specified, the distribute list applies to routes redistributed from that source. Only routes that pass the distribute list are redistributed. The protocol value may be either rip or ospf.

Default Configuration

No distribute lists are defined by default.

Command Mode

BGP Router Configuration mode

User Guidelines

Only one instance of this command may be defined for each route source (RIP, OSPF, static, connected). One instance of this command may also be configured as a global filter for outbound prefixes.

If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

When a distribute list is added, changed, or deleted for route redistribution, BGP automatically reconsider all best routes.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-router)#distribute-list prefix 255 out

distribute-list prefix out (IPv6 Address Family Configuration)

Use this command to apply an IPv6 prefix list to IPv6 routes advertised via BGP.
Syntax

distribute-list prefix list-name out [ protocol | connected | static ]

no distribute-list prefix list-name out [ protocol | connected | static ]

- prefix list-name—A prefix list used to filter routes advertised to neighbors.
- protocol|connected|static—(Optional) When a route source is specified, the distribute list applies to routes redistributed from that source. Only routes that pass the distribute list are redistributed. The protocol value may be either rip or ospf.

Default Configuration

No distribute lists are defined by default.

Command Mode

IPv6 Address Family Configuration mode

User Guidelines

Only one instance of this command may be defined for each route source (RIP, OSPF, static, connected). One instance of this command may also be configured as a global filter for outbound prefixes.

If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

When a distribute list is added, changed, or deleted for route redistribution, BGP automatically reconsiders all best routes.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console(config-router-af)#distribute-list prefix 255 out

enable

This command globally enables BGP, while retaining the configuration.
**Syntax**

enable
no enable

**Default Configuration**

By default, BGP is enabled once the administrator has specified the local AS number with the `router bgp` command and configured a router id with `bgp router-id`.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

When disabling BGP using `no enable`, BGP retains its configuration. The `no router bgp` command resets all BGP configuration to default values.

When BGP is administratively disabled, BGP sends a NOTIFICATION message to each peer with a Cease error code.

The `no enable` command persists in the running-config (and startup-config) only when a router-id has assigned using the `bgp router-id` command. If no router-id has been assigned, the administrative state will not appear in the running-config or in the startup-config.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#enable
```

### ip as-path access-list

Use this command to create an AS path access list. To delete an AS path access list, use the `no` form of this command.

**Syntax**

```
ip as-path access-list as-path-list-number { permit | deny } regexp
```
no ip as-path access-list as-path-list-number

- as-path-list-number—A number from 1 to 500 uniquely identifying the list. All AS path access list commands with the same as-path-list-number are considered part of the same list.
- permit—Permit routes whose AS Path attribute matches the regular expression.
- deny—Deny routes whose AS Path attribute matches the regular expression.
- regexp—A regular expression used to match the AS path attribute of a BGP path where the AS path is treated as an ASCII string.

Default Configuration
No AS path lists are configured by default. There are no default values for any of the parameters of this command.

Command Mode
Global Configuration mode

User Guidelines
An AS path access list filters BGP routes on the AS path attribute of a BGP route. The AS path attribute is a list of the autonomous system numbers along the path to the destination. An AS path access list is an ordered sequence of statements. Each statement specifies a regular expression and a permit or deny action. If the regular expression matches the AS path of the route expressed as an ASCII string, the route is considered a match and the statement’s action is taken. An AS path list has an implicit deny statement at the end. If a path does not match any of the statements in an AS path list, the action is considered to be deny.

Once an path list is created, individual statements cannot be deleted from it. To remove an individual statement, delete the AS path list and recreate it without the statement to be deleted.

Statements are applied in the order in which they are created. New statements are added to the end of the list. The statement with the first matching regular expression is applied.
Up to 128 AS path access lists can be configured, with up to 64 statements each. To enter the question mark within a regular expression, first enter CTRL-V to prevent the CLI from interpreting the question mark as a request for help.

<table>
<thead>
<tr>
<th>Special Character/Symbol</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>asterisk</td>
<td>*</td>
</tr>
<tr>
<td>brackets</td>
<td>[]</td>
</tr>
<tr>
<td>caret</td>
<td>^</td>
</tr>
<tr>
<td>dollar sign</td>
<td>$</td>
</tr>
<tr>
<td>hyphen</td>
<td>-</td>
</tr>
<tr>
<td>period</td>
<td>.</td>
</tr>
<tr>
<td>plus sign</td>
<td>+</td>
</tr>
<tr>
<td>question mark</td>
<td>?</td>
</tr>
<tr>
<td>underscore</td>
<td>_</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

In the following example, the router is configured to reject routes received from neighbor 172.20.1.1 with an AS path that indicates the route originates in or passes through AS 100.

```
console(config)# ip as-path access-list 1 deny _100_
console(config)# ip as-path access-list 1 deny ^100$ 
console(config)# router bgp 1
```
ip bgp-community new-format

Use this command to display BGP standard communities in AA:NN format. To display BGP standard communities as 32-bit integers, use the no form of this command.

**Syntax**

```plaintext
ip bgp-community new-format
no ip bgp-community new-format
```

**Default Configuration**

Standard communities are displayed in AA:NN format.

**Command Mode**

Global Configuration mode

**User Guidelines**

RFC 1997 specifies that the first two bytes of a community number are considered to be an autonomous system number. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```plaintext
console(config)# ip bgp-community new-format
```

---

**ip bgp fast-external-fallover**

Use the `ip bgp fast-external-fallover` command to configure fast external failover behavior for a specific routing interface.

**Syntax**

```plaintext
ip bgp fast-external-fallover { permit | deny }
```
no ip bgp fast-external-fallover

- **permit**—Enables fast external fallover on the interface, regardless of the global configuration of the feature.
- **deny**—Disables fast external fallover on the interface, regardless of the global configuration of the feature.

**Default Configuration**

Fast external fallover is enabled globally by default. There is no default interface configuration.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

This command overrides for a specific routing interface the fast external fallover behavior configured globally. If **permit** is specified, the feature is enabled on the interface, regardless of the global configuration. If **deny** is specify, the feature is disabled on the interface, regardless of the global configuration. The command **no ip bgp fast-external-fallover** clears the interface settings and indicates that the global settings should be used.

**Example**

```
console(config-if-vlan1)#ip bgp fast-external-fallover permit
```

**ip community-list**

Use this command to create or configure a BGP community list. To delete a community list, use the **no** form of this command.

**Syntax**

```
ip community-list standard list-name {permit | deny} [community-number] [no-advertise] [no-export] [no-export-subconfed] [no-peer]

no ip community-list standard list-name
```

- **standard** list-name—Identifies a named standard community list. The name may contain up to 32 characters.
- **permit**—Indicates that matching routes are permitted.
• **deny**—Indicates that matching routes are denied.

• **community-number**—From zero to sixteen community numbers formatted as a 32-bit integers or in AA:NN format, where AA is a 2-byte autonomous system number and NN is a 16 bit integer. The range is 1 to 4,294,967,295 (any 32-bit integer other than 0). Communities are separated by spaces.

• **no-advertise**—The well-known standard community: NO_ADVERTISE (0xFFFFFF02), which indicates the community is not to be advertised.

• **no-export**—The well-known standard community: NO_EXPORT, (0xFFFFFF01), which indicates the routes are not to be advertised outside the community.

• **no-export-subconfed**—The well-known standard community: NO_EXPORT_SUBCONFED (0xFFFFFF03), which indicates the routes are not to be advertised to external BGP peers.

**Default Configuration**

No community lists are configured by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

A community list statement with no community values is considered a match for all routes, regardless of their community membership. So the statement

```
ip community-list bullseye permit
```

is a “permit all” statement.

A community number may be entered in either format, as a 32-bit integer or a pair of 16-bit integers separated by a colon, regardless of whether the `ip bgp-community new-format` command is active. Up to 16 communities, including the well-known communities, can be listed in a single command. Up to 32 statements may be configured with a given community list name. Up to 128 unique community list names may be configured.

Successive invocations of the command are additive in that they add to the configured communities up to the maximum.
If more than the maximum allowed communities are configured, the excess entries are ignored.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config)# ip community-list standard test permit
```

**`ip extcommunity-list`**

Use the `ip extcommunity-list` command to create an extended community list to configure VRF route filtering. Use the `no` form of the command to configure VRF route filtering.

**Syntax**

```
ip extcommunity-list standard-list [permit | deny][rt value] [soo value]
no ip extcommunity-list standard-list
```

- **standard-list** — A standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.
- **permit | deny**— Permits or denies access for a matching condition. Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.
- **rt value**— Specifies the route target (RT) extended community value. The route target can be configured only with standard extended community lists. This value can be entered in one of the following formats:
  - 16-bit AS number :a 32-bit value (Ex : 100:11)
  - 32-bit IPv4 address :a 16-bit value (Ex : 10.1.1.1:22)
- **soo value**— Specifies the site of origin (SOO) extended community value. The site of origin can be configured only with standard extended community lists. This value can be entered in one of the following formats:
  - 16-bit AS number :a 32-bit value (Ex : 100:11)
  - 32-bit IPv4 address :a 16-bit value (Ex : 10.1.1.1:22)
Default Configuration

No subnets are associated with a BGP listen subnet range, and the BGP dynamic neighbor feature is not activated.

Command Mode

Global Config mode

User Guidelines

This command is used to configure numbered extended community lists. Extended community attributes are used to filter routes for VRFs. All the standard rules of access lists apply to the configuration of extended community lists. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists.

Once the first permit/deny clause has been entered for a community list, subsequent permit/deny clauses with the same list identifier are appended to the end of the list.

Expanded community list and regular expressions are not supported.

Route Target Extended Community Attribute

The route target (RT) extended communities attribute is configured with the `rt` keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

Site of Origin Extended Community Attribute

The site of origin (SOO) extended communities attribute is configured with the `soo` keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multi-homed. The SOO extended community attribute is configured using a route map in both outbound and inbound directions. The SOO should not be configured for stub sites or sites that are not multi-homed.
**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example shows the creation of an extended community list that permits routes from route target 1:1 and site of origin 2:2 and denies routes from route target 3:3 and 4:4.

(R1) (Config)# ip extcommunity-list 10 permit rt 1:1
(R1) (Config)# ip extcommunity-list 10 permit rt 2:2
(R1) (Config)# ip extcommunity-list 20 deny rt 3:3 rt 4:4

List 10 shows a logical OR condition which means the first match is processed.

List 20 shows a logical AND condition which means all the community values must match in order for list 20 to be processed.

The following example show how the extended communities list is used by route-maps.

(R1) (config)# route-map SEND_OUT permit 10
(R1) (config-route-map)# match extcommunity 10
(R1) (config-route-map)# set extcommunity rt 10:10 additive
(R1) (config-route-map)# exit

The following example shows the usage of extended communities attribute in BGP configuration mode and sending of the extended communities attribute to external peer at 1.1.1.1.

(R1) (Config)# router bgp 1
(R1) (Config-router)# neighbor 1.1.1.1 remote-as 2
(R1) (Config-router)# neighbor 1.1.1.1 route-map SEND_OUT out
(R1) (Config-router)# address-family vpnv4 unicast
(R1) (Config-router-af)# neighbor 1.1.1.1 send-community extended
(R1) (Config-router-af)# neighbor 1.1.1.1 activate

**match extcommunity**

Use the `match extcommunity` command to match BGP extended community list attributes. Use the `no` form of this command to remove the match extcommunity from the configuration and BGP extended community list attribute entry.

⚠️ **NOTE:** This command is effective only if BGP is running on the router.
Syntax
match extcommunity standard-list
no match extcommunity standard-list
  • standard-list—A standard list identifier that identifies one or more permit
or deny groups of extended communities. The range is from 0–100.

Default Configuration
BGP extended community list attributes are not matched.

Command Mode
Route Map Configuration mode

User Guidelines
The match extcommunity command is used to configure match clauses that
use extended community attributes in route maps. All the standard rules of
match and set clauses apply to the configuration of extended community
attributes.

Command History
Introduced in version 6.3.0.1 firmware.

Example
The following example shows that the routes that match extended
community list 10 will set the additional route target attribute to 10:10.

(R1)(config)# ip extcommunity-list 10 permit rt 1:1
(R1)(config)# route-map SEND_OUT permit 10
(R1)(config-route-map)# match extcommunity 10
(R1)(config-route-map)# set extcommunity rt 10:10 additive
(R1)(config-route-map)# exit

maximum-paths (BGP Router Configuration)
Use this command to specify the maximum number of next hops BGP may
include in an Equal Cost Multipath (ECMP) route derived from paths
received from neighbors outside the local autonomous system.
Syntax
maximum-paths number-of-paths
no maximum-paths
  • number-of-paths—The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or currently selected SDM template further restricts the range.

Default Configuration
BGP advertises a single next hop by default.

Command Mode
BGP Router Config

User Guidelines
Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Refer to Appendix A-1 in the Users Configuration Guide for the default per platform ECMP ranges using the entry “Number of ECMP next hops per route.” The number of ECMP next hops is dependent on the chosen STM template and may be greater or lesser than the default. Use the show sdm prefer command to display the ECMP Next Hops for the currently selected template.

Command History
Introduced in version 6.2.0.1 firmware.

Example
consloe(config-router)#maximum-paths 5
maximum-paths (IPv6 Address Family Configuration)

Use this command to limit the number of ECMP next hops in IPv6 routes from external peers.

**Syntax**

maximum-paths number-of-paths

no maximum-paths

• number-of-paths—The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

**Default Configuration**

BGP advertises a single next hop by default.

**Command Mode**

IPv6 Address Family Configuration

**User Guidelines**

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

The following ranges are supported:

• N40xx—1-4
• N30xx—1-16
• N20xx—1-1

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

console(config-router-af)#maximum-paths 5
maximum-paths ibgp (BGP Router Configuration)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Syntax

maximum-paths ibgp number-of-paths
no maximum-paths ibgp

- number-of-paths—The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default Configuration

BGP uses a single next hop by default.

Command Mode

BGP Router Configuration mode

User Guidelines

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, and IGP distance) and the paths are received from different routers. When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

The following ranges are supported in the default SDM template:

- N40xx 1-4
- N30xx 1-4
- N20xx 1-1

Configure the data-center version of the desired SDM template to increase the ECMP paths.

Command History

Introduced in version 6.2.0.1 firmware.
**Example**

```plaintext
console(config-router)#maximum-paths ibgp 5
```

**maximum-paths ibgp (IPv6 Address Family Configuration)**

Use this command to limit the number of ECMP next hops in IPv6 routes from internal peers.

**Syntax**

```plaintext
maximum-paths ibgp number-of-paths
no maximum-paths ibgp
```

- **number-of-paths**—The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

**Default Configuration**

BGP uses a single next hop by default.

**Command Mode**

IPv6 Address Family Configuration mode

**User Guidelines**

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, and IGP distance) and the paths are received from different routers. When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

The following ranges are supported in the default SDM template:

- **N40xx** 1-4
- **N30xx** 1-4
- **N20xx** 1-1

Configure the data-center version of the desired SDM template to increase the ECMP paths.
**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config-router-af)#maximum-paths ibgp 5
```

**neighbor activate**
Use this command to enable the exchange of IPv6 routes with a neighbor. To disable the exchange of IPv6 addresses, use the **no** form of this command.

**Syntax**
```
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } activate
no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } activate
```

- **ip-address**—The IP address of a peer.
- **ipv6-address**—The IPv6 address of a peer.
- **interface-id** — If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. This must be a VLAN routing interface and is specified using the VLAN keyword.
- **autodetect interface interface-id**—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface. Range is 1–4093.

**Default Configuration**
The exchange of IPv6 routes is disabled by default.

**Command Mode**
IPv4 Address Family Configuration mode, IPv6 Address Family Configuration mode

**User Guidelines**
The neighbor address must be the same IP address used in the neighbor remote-as command to create the peer.
When IPv6 is enabled or disabled for a neighbor, the adjacency is brought down and restarted to communicate to the change to the peer. Completely configure IPv6 policy for the peer before activating the peer.

**Command History**

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

**Example**

The following example enables the exchange of IPv6 routes with the external peer at 172.20.1.2 and sets the next hop for IPv6 routes sent to that peer.

```
console (config)# router bgp 1
console (config-router)# neighbor 172.20.1.2 remote-as 2
console (config-router)# address-family ipv6
console (Config-router-af)# neighbor 172.20.1.2 activate
console (Config-router-af)# neighbor 172.20.1.2 route-map SET-V6-NH out
console (Config-router-af)# exit
console (config-router)# exit
console (config)# route-map SET-V6-NH permit 10
console (route-map)# set ipv6 next-hop 2001:1:200::1
```

**neighbor advertisement-interval (BGP Router Configuration)**

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor.

**Syntax**

```
neighbor { ip-address [interface interface-id]} advertisement-interval seconds
no neighbor { ip-address [interface interface-id]} advertisement-interval
```

- **interface-id**—A routing interface identifier.
- **ip-address**—The neighbor’s IPv4 address.
- **seconds**—The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.
**Default Configuration**

The default value is 30 seconds for external peers and 5 seconds for internal peers.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

Dell EMC Networking BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```plaintext
console(config-router)# neighbor 10.27.9.99 advertisement-interval 100
```

### neighbor advertisement-interval (IPv6 Address Family Configuration)

In IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes.

**Syntax**

```plaintext
neighbor { ipv6-address [interface interface-id]} advertisement-interval seconds

no neighbor { ipv6-address [interface interface-id]} advertisement-interval
```

- `interface-id`—A routing interface identifier.
ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.

seconds—The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

Default Configuration
The default value is 30 seconds for external peers and 5 seconds for internal peers.

Command Mode
IPv6 Address Family Configuration mode

User Guidelines
RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

Dell EMC Networking BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements. The VLAN interface must also be specified if a link-local address is specified.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router-af)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 advertisement-interval 50

neighbor allowas-in
Use the neighbor allowas-in command to accept prefixes even if local ASN is part of the AS_PATH attribute. Use the no form of the command to disable acceptance of prefixes if the local ASN is part of the AS_PATH.
**Syntax**

```plaintext
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect
interface vlan vlan-id } allowas-in count
no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect
interface interface-id } allowas-in
```

- **interface-id** — A routing interface identifier beginning with the VLAN keyword.
- **ip-address** — The neighbor’s IPv4 address.
- **ipv6-address [ interface interface-id ]** — The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- **autodetect interface interface-id** — The VLAN routing interface on which the neighbor’s link local IPv6 address is auto detected. Use the `vlan` keyword and a VLAN identifier.
- **allowas-in count** — The maximum number of occurrences of the local ASN allowed in the AS_PATH attribute received in the prefix updates. The allowed range is `<1-10>`.

**Default Configuration**

The router does not accept prefixes with the local ASN is part of the AS_PATH attribute.

**Command Mode**

BGP Router Configuration mode, IPv4 Address Family Configuration mode

**User Guidelines**

A neighbor can inherit this configuration from a peer template.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console(config)# router bgp 65000
console(config-router)# neighbor 172.20.1.2 remote-as 65001
console(config-router)# neighbor 172.20.1.2 allowas-in 1
```
console(config-router)# neighbor 2001::2 remote-as 65003
console(config-router)# neighbor 2001::2 allowas-in 3

**neighbor connect-retry-interval**

Use this command in to configure the initial connection retry time for a specific neighbor.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id} connect-retry-interval retry-time

no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id} connect-retry-interval
```

- *ip-address*—The neighbor’s IPv4 address.
- *ipv6-address*—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. The interface must be a VLAN routed interface.
- *interface interface-id*—A routing interface identifier (VLAN identifier).
- *autodetect interface interface-id*—The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface must be a VLAN routed interface.
- *retry-time*—The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

**Default Configuration**

The default value is 2 seconds.

**Command Mode**

BGP Router Configuration mode
IPv4 Address Family Configuration mode

**User Guidelines**

If a neighbor does not respond to an initial TCP connection attempt, the N3000/N5100/N4000 Series switch retries three times. The first retry is after the retry interval configured with `neighbor connect-retry-interval`. Each
subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt. The VLAN interface must also be specified if a link-local address is specified.

Command History
Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

Example
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10
connect-retry-interval 10

neighbor default-originate (BGP Router Configuration)

To configure BGP to originate a default route to a specific neighbor, use the neighbor default-originate command in BGP Router Configuration mode.

Syntax
neighbor { ip-address | ipv6-address [interface interface-id]} default-originate [route-map map-name]

- interface-id—A routing interface identifier (VLAN interface).
- ip-address—The neighbor’s IPv4 address.
- ipv6-address —The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- map-name—(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default Configuration
No default is originated by default.
**Command Mode**

BGP Router Configuration mode

**User Guidelines**

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the default-information originate (BGP Router Configuration) command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the show ip bgp command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the show ip bgp neighbors advertised-routes command).

Origination of the default route is not subject to a prefix filter configured with the command distribute-list prefix out (BGP Router Configuration).

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a match ip-address term, that term is ignored. If the route map includes match community or match as-path terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised. The VLAN interface must also be specified if a link-local address is specified.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 default-originate
```

**neighbor default-originate (IPv6 Address Family Configuration)**

To configure BGP to originate a default IPv6 route to a specific neighbor, use the neighbor default-originate command in IPv6 Address Family configuration mode.
Syntax

```
neighbor { ip-address | ipv6-address [interface interface-id]} default-originate [route-map map-name]
```

- interface-id—A routing interface identifier (VLAN interface).
- ip-address—The neighbor’s IPv4 address.
- ipv6-address —The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- map-name—(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default Configuration

No default is originated by default.

Command Mode

IPv6 Address Family Configuration

User Guidelines

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the `default-information originate (BGP Router Configuration)` command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the `show ip bgp` command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the `show ip bgp neighbors advertised-routes` command).

Origination of the default route is not subject to a prefix filter configured with the command `distribute-list prefix out (BGP Router Configuration)`.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a `match ip-address` term, that term is ignored. If the route map includes `match community` or `match as-path`
terms, the default route is not advertised. If there is no route map with the
route map name given, the default route is not advertised. The VLAN
interface must also be specified if a link-local address is specified.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router-af)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 default-originate
```

**neighbor description**

Use this command to record a text description of a neighbor. The description
is informational and has no functional impact.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect
interface interface-id } description text
```

```
no neighbor { ip-address | ipv6-address [ interface interface-id ] autodetect
interface interface-id } description
```

- **interface-id**—A routing interface identifier (VLAN interface).
- **ip-address**—The neighbor’s IP address.
- **ipv6-address [ interface interface-id ]**—The neighbor’s IPv6 address. If the
  neighbor’s IPv6 address is a link local address, the local interface must also
  be specified. The interface-id must specify a routing interface identifier
  (VLAN ID).
- **text**—Text description of neighbor. Up to 80 characters are allowed.
- **autodetect interface interface-id**—(Optional) The routing interface on
  which the neighbor’s link local IPv6 address is auto detected. The
  interface-id must be a VLAN routing interface.

**Default Configuration**

No description is configured by default.
**Command Mode**

BGP Router Configuration mode  
IPv4 Address Family Configuration mode

**User Guidelines**

The VLAN interface must also be specified if a link-local address is specified.

**Command History**

Introduced in version 6.2.0.1 firmware.  
Updated in version 6.3.0.1 firmware.

**Example**

console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10  
description Test-System

**neighbor ebgp-multihop**

Use the `neighbor ebgp-multihop` command to configure BGP to form neighborship with external peers that are not directly connected.

**Syntax**

```text
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } ebgp-multihop hop-count
```

```text
no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } ebgp-multihop hop-count
```

- ip-address — The neighbor’s IPv4 address. This is the IP address of the neighbor on the connected link.
- ipv6-address — The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. Valid in IPv6 address family configuration mode.
- interface interface-id — The local VLAN routing interface over which the IPv6 neighbor can be reached or is auto-detected. Use the vlan keyword and a VLAN ID. Range 1-4093.
Layer 3 Routing Commands

- **autodetect interface interface-id** — The VLAN routing interface on which the neighbor’s link local IPv6 address is auto detected. Use the vlan keyword and a VLAN ID. Range 1-4093.

- **hop-count** — The maximum hop-count allowed to reach the neighbor. The allowed range is 1–255.

**Default Configuration**

The default hop count is 64.

**Command Mode**

BGP Router Configuration mode, IPv6 Address Family Configuration mode

**User Guidelines**

The ebgp-multihop parameter is relevant only for external BGP neighbors. For internal BGP neighbors, the TTL value remains 64 and can’t be modified. A neighbor can inherit this configuration from a peer template. To make the update-source config work for external BGP neighbors, `ebgp-multihop hop-count` should be configured to a TTL value larger than the default TTL of 1.

**Autodetect Interface**

When BGP is deployed in an IPv6 data center network, it is desirable to use IPv6 link local addresses as BGP neighbors. Using link local addresses avoids the need to assign and manage global IPv6 addresses on interconnect links.

Dell EMC Networking already supports BGP neighbors with link local IPv6 addresses, but it requires that the link local IPv6 address of the neighbor be configured using the BGP “neighbor” command. Since the link local address is derived from the switch MAC address, the network administrator needs to know the MAC address of all the switches deployed in the network, and if one switch fails and is replaced with a different switch then all the BGP neighbor switches need to be reconfigured to change the link local address specified in their neighbor commands.

The IPv6 Link Local Address Auto Detect feature eliminates the need for the network administrator to configure the link local IPv6 address of every neighbor. Instead of specifying the link local IPv6 address, the network administrator...
administrator can use a special keyword “autodetect” to refer to the link local IPv6 address of the neighbor. For example: “neighbor autodetect interface 0/21 remote-as 10000”

There are several restrictions to this feature:

1. The “interface” can only refer to non-multiple access VLAN routing interfaces. It does not work on tunnels.
2. Only one “autodetect” neighbor can be configured per interface.
3. If autodetect neighbor is configured on an interface, a link-local IPv6 neighbor cannot be configured on the same interface.
4. If more than one link local IPv6 address is detected on the specified interface, this is considered to be an error and the address auto-detection fails.
5. The feature is supported only on platforms that also support the RFC 5549.
6. The feature is applicable only for directly connected neighbors.
7. Multiple access VLANs are not supported.

Command History
Introduced in version 6.3.0.1 firmware.

Example

```
console(config)# router bgp 65000
console(config-router)# neighbor 172.20.1.2 remote-as 65001
console(config-router)# neighbor 172.20.1.2 ebgp-multihop 3
console(config-router)# neighbor 2001::2 remote-as 65003
console(config-router)# neighbor 2001::2 ebgp-multihop 4
```

neighbor filter-list (BGP Router Configuration)

This command filters advertisements to or from a specific neighbor according to the advertisement’s AS Path.

Syntax

```
neighbor { ip-address | ipv6-address [ interface interface-id ]} filter-list as-path-list-number {in | out}
```
no neighbor { ip-address | ipv6-address [ interface interface-id ]} filter-list as-path-list-number {in | out}

- interface-id—A routing interface identifier (VLAN interface).
- ip-address—The neighbor’s IPv4 address.
- ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- as-path-list-number—Identifies an AS path list.
- in—The AS Path list is applied to advertisements received from the neighbor.
- out—The AS Path list is applied to advertisements to be sent to the neighbor.

Default Configuration
No neighbor filter lists are configured by default.

Command Mode
BGP Router Configuration mode

User Guidelines
Only a single AS path list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS path list number replaces the previous AS path list number.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered. The VLAN interface must also be specified if a link-local address is specified.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 filter-list 1 in
**neighbor filter-list (IPv6 Address Family Configuration)**

This command filters BGP to apply an AS path access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both IPv4 and IPv6 NLRI, it could be filtered for IPv4 but accepted for IPv6 or vice versa.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ]} filter-list as-path-list-number { in | out }
no neighbor { ip-address | ipv6-address [ interface interface-id ]} filter-list as-path-list-number { in | out }
```

- **ip-address** — The neighbor’s IPv4 address.
- **ipv6-address [ interface interface-id ]** — The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- **as-path-list-number** — Identifies an AS path list.
- **in** — The AS Path list is applied to advertisements received from the neighbor.
- **out** — The AS Path list is applied to advertisements to be sent to the neighbor.

**Default Configuration**

No neighbor filter lists are configured by default.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered. The VLAN interface must also be specified if a link-local address is specified.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router-af)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 filter-list 1 in
```

**neighbor inherit peer**

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the `neighbor inherit peer` command. To remove the inheritance, use the `no` form of this command.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } inherit peer template-name
```

```
no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } inherit peer template-name
```

- **ip-address**—The neighbor’s IPv4 address.
- **ipv6-address [interface interface-id]**—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- **autodetect interface interface-id** – The VLAN routing interface on which the neighbor’s link local IPv6 address is auto detected.
- **template-name**—The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

**Default Configuration**

No peer configuration parameters are inherited by default.

**Command Mode**

BGP Router Configuration mode, IPv4 Address Family Configuration mode
User Guidelines

Neighbor session and policy parameters can be configured once in a peer template and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbor can inherit directly from only one peer template.

Command History

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

Example

console(config)# router bgp 65000
console(config-router)# neighbor 172.20.1.2 remote-as 65001
console(config-router)# neighbor 172.20.2.2 remote-as 65001
console(config-router)# template peer AGGR
console(config-rtr-tmp)# timers 3 9
console(config-rtr-tmp)# address-family ipv4
console(config-rtr-tmp-af)# send-community
console(config-rtr-tmp-af)# route-map RM4-IN in
console(config-rtr-tmp-af)# route-map RM4-OUT out
console(config-rtr-tmp-af)# exit
console(config-rtr-tmp)# exit
console(config-router)# neighbor 172.20.1.2 inherit peer AGGR
console(config-router)# neighbor 172.20.2.2 inherit peer AGGR

neighbor local-as

Use the neighbor local-as command to configure BGP to advertise the local-as instead of the router’s own AS in the routes advertised to the neighbor.

Syntax

neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface vlan vlan-id } local-as as-number no-prepend replace-as no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } local-as

• interface-id—A routing interface identifier (VLAN interface).
• ip-address — The neighbor’s IPv4 address.
• **ipv6-address [ interface interface-id]** — The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.

• **autodetect interface interface-id** — The VLAN routing interface on which the neighbor’s link local IPv6 address is auto detected.

• **local-as as-number** — The AS number to advertise as the local AS in the AS PATH sent to the neighbor.

• **no-prepend** — The local-as is not prepended in the AS PATH received in the updates from this neighbor.

• **replace-as** — Replace the router’s own AS with the local-as in the AS PATH sent to the neighbor.

**Default Configuration**

No local-as is configured for any peer.

**Command Mode**

BGP Router Configuration mode, IPv4 Address Family Configuration mode

**User Guidelines**

In typical data center deployments using CLOS networks, the peering is all external BGP between the BGP devices requiring an unique ASN for each router. Normally, the private BGP networks are expected to use private AS numbers. But, there are only 1024 private AS numbers in the standard 2-byte ASN.

Due to this limitation, data center deployments are forced to use public ASNs in their private networks. When such private networks are interconnected to each other, there needs to be a way to manipulate the public ASNs in the route advertisements so that the private networks with the public ASNs don’t experience ASN conflicts.

With the options no-prepend and replace-as

• The router replaces the global AS of the router with the configured local-as when advertising the routes to the peer on which this command is configured.

• As well the local-as is not prepended to the routes received from the neighbor on which this command is configured.
This command is allowed only on external BGP neighbors. A neighbor can inherit this configuration from a peer template.
When the local-as is configured for a peer, the BGP peer adjacency gets reset.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
```
console(config)#router bgp 65000
console(config-router)# neighbor 172.20.1.2 remote-as 65001
console(config-router)# neighbor 172.20.1.2 local-as 65002 no-prepend replace-as
console(config-router)# neighbor 2001::2 remote-as 65003
console(config-router)# neighbor 2001::2 local-as 65002 no-prepend replace-as
```

**neighbor maximum-prefix (BGP Router Configuration)**

Use the `neighbor maximum-prefix` command to configure the maximum number of IPv4 prefixes that BGP will accept from a specified neighbor.

**Syntax**
```
neighbor { ip-address | ipv6-address [ interface interface-id ]} maximum-prefix { maximum [threshold] [warning-only] | unlimited }
no neighbor { ip-address | ipv6-address [ interface interface-id ]} maximum-prefix
```

- **ip-address**—The neighbor’s IP address.
- **ipv6-address**—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- **interface-id**—If the neighbor’s IPv6 address is a link local address, the local VLAN routing interface must also be specified.
- **maximum**—The maximum number of prefixes BGP will accept from this neighbor. Range 0-4294967295. Values greater than the free space in the route table are not enforced.
• **threshold**—The percentage of the maximum number of prefixes BGP configured for this neighbor. When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%. Unless warning-only is specified, BGP shuts down the adjacency when the threshold is reached.

• **unlimited**—Do not enforce any prefix limit. Use this option when inbound filtering will reduce the number received prefixes such that they will fit in the routing table. Exceeding the capacity of the routing table will cause the adjacency to be shut down unless the warning-only option is configured.

• **warning-only**—(Optional) If BGP receives more than the maximum number of prefixes, BGP writes a log message rather than shutting down the adjacency.

**Default Configuration**

There is no prefix limit by default. The default warning threshold is 75%. A neighbor that exceeds the limit is shut down by removing the adjacency unless the **warning-only** option is configured.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

If the peering session is shut down, the adjacency stays down until **clear ip bgp** is issued for the neighbor.

Different limits can be set for IPv4 and IPv6. The VLAN interface must also be specified if a link-local address is specified.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10
maximum-prefix unlimited
```
neighbor maximum-prefix (IPv6 Address Family Configuration)

In IPv6 address family configuration mode, the `neighbor maximum-prefix` command specifies the maximum number of IPv6 prefixes that BGP will accept from a given neighbor.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ]} maximum-prefix { maximum [threshold] [warning-only] | unlimited }
no neighbor { ip-address | ipv6-address [ interface interface-id ]} maximum-prefix
```

- **ip-address**—The neighbor’s IP address.
- **ipv6-address**—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- **interface-id**—If the neighbor’s IPv6 address is a link local address, the local VLAN routing interface must also be specified.
- **maximum**—The maximum number of prefixes BGP will accept from this neighbor. Range 0-4294967295. Values greater than the free space in the route table are not enforced.
- **threshold**—The percentage of the maximum number of prefixes BGP configured for this neighbor. When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%. Unless warning-only is specified, BGP shuts down the adjacency when the threshold is reached.
- **unlimited**—Do not enforce any prefix limit. Use this option when inbound filtering will reduce the number received prefixes such that they will fit in the routing table. Exceeding the capacity of the routing table will cause the adjacency to be shut down unless the warning-only option is configured.
- **warning-only**—(Optional) If BGP receives more than the maximum number of prefixes, BGP writes a log message rather than shutting down the adjacency.
**Default Configuration**

There is no prefix limit by default. The default warning threshold is 75%. A neighbor that exceeds the limit is shut down by removing the adjacency unless the `warning-only` option is configured.

**Command Mode**

IPv6 Address Family Configuration mode

**User Guidelines**

If the peering session is shut down, the adjacency stays down until `clear ip bgp` is issued for the neighbor.

Different limits can be set for IPv4 and IPv6. In IPv6 address family mode, the command accepts either an IPv4 or an IPv6 address. The VLAN interface must also be specified if a link-local address is specified.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router-af)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 maximum-prefix unlimited
```

**neighbor next-hop-self (BGP Router Configuration)**

The `neighbor next-hop-self` command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP retains the next hop attribute received from the external peer.

**Syntax**

```
neighbor { ip-address | ipv6-address [ interface interface-id ]} next-hop-self
no neighbor { ip-address | ipv6-address [ interface interface-id ]} next-hop-self
```

- `ip-address` – The neighbor’s IPv4 address.
Layer 3 Routing Commands

- ipv6-address [ interface interface-id ] – The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.

Default Configuration
This is not enabled by default.

Command Mode
BGP Router Configuration mode

User Guidelines
When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer’s IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or “DMZ”) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP. The neighbor next-hop-self command sets the next hop for all routes sent to a neighbor. The VLAN interface must also be specified if a link-local address is specified.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 next-hop-self

neighbor next-hop-self (IPv6 Address Family Configuration)
In IPv6 address family configuration mode, the neighbor next-hop-self command configures BGP to use a local address as the IPv6 next hop when advertising IPv6 routes to a specific peer.

Syntax
neighbor { ip-address | ipv6-address [ interface interface-id ]} next-hop-self
no neighbor { ip-address | ipv6-address [ interface interface-id ]} next-hop-self
  • ip-address – The neighbor’s IPv4 address.
  • ipv6-address [ interface interface-id ] – The neighbor’s IPv6 address. If the
    neighbor’s IPv6 address is a link local address, the local interface must also
    be specified.

Default Configuration
This is not enabled by default.

Command Mode
IPv6 Address Family Configuration mode

User Guidelines
When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer’s IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or “DMZ”) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

In IPv6 Address Family Configuration mode, the command accepts either an IPv4 or an IPv6 address. For IPv6, BGP uses an IPv6 address from the local interface that terminates the peering session. The VLAN interface must also be specified if a link-local address is specified.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router-af)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 next-hop-self

neighbor password
Use the neighbor password command to enable MD5 authentication of TCP segments sent to and received from a neighbor, and to configure an authentication key.
Syntax

neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } password string

no neighbor { ip-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } password

• ip-address—The neighbor’s IPv4 address.
• ipv6-address [ interface interface-id ]—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. The interface-id must specify a routing interface identifier (VLAN ID).
• autodetect interface interface-id—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface.
• string—Case-sensitive password from 1 to 25 characters in length.

Default Configuration

MD5 authentication is disabled by default.

Command Mode

BGP Router Configuration mode
IPv4 Address Family Configuration mode

User Guidelines

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. Using the default hold times, both passwords must be changed within 120 seconds to guarantee the connection is not dropped. The VLAN interface must also be specified if a link-local address is specified.

Command History

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.
neighbor prefix-list (BGP Router Configuration)

Use the neighbor prefix-list command to filter advertisements sent to a specific neighbor based on the destination prefix of each route.

Syntax

neighbor { ip-address | ipv6-address [interface vlan vlan-id]} prefix-list
prefix-list-name { in | out }

no neighbor { ip-address | ipv6-address [interface vlan vlan-id]} prefix-list
prefix-list-name { in | out }

- ip-address—The neighbor’s IPv4 address.
- prefix-list-name—The name of an IP prefix list.
- ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. This command is available in IPv6 address family mode.
- interface vlan vlan-id—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range: 1-4093.
- in—Apply the prefix list to advertisements received from this neighbor.
- out—Apply the prefix list to advertisements to be sent to this neighbor.

Default Configuration

No prefix list is configured.

Command Mode

BGP Router Configuration mode

User Guidelines

Only one prefix list may be defined for each neighbor in each direction. If a prefix list that does not exist is assigned, all prefixes are permitted. The VLAN interface must also be specified if a link-local address is specified.
Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#neighbor FE80::0202:B3FF:FE1E:8329 interface vlan 10 prefix-list test in

neighbor prefix-list (IPv6 Address Family Configuration)
In IPv6 address family configuration mode, the neighbor prefix-list command specifies an IPv6 prefix list to filter routes received from or advertised to a given peer.

Syntax
neighbor { ip-address | ipv6-address [interface vlan vlan-id]} prefix-list prefix-list-name { in | out }
no neighbor { ip-address | ipv6-address [interface vlan vlan-id]} prefix-list prefix-list-name { in | out }

- ip-address—The neighbor’s IPv4 address.
- prefix-list-name—The name of an IP prefix list.
- ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. This command is available in IPv6 address family mode.
- interface vlan vlan-id—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range: 1-4093.
- in—Apply the prefix list to advertisements received from this neighbor.
- out—Apply the prefix list to advertisements to be sent to this neighbor.

Default Configuration
No prefix list is configured.

Command Mode
IPv6 Address Family Configuration mode
**User Guidelines**

Only one prefix list may be defined for each neighbor in each direction. If a prefix list that does not exist is assigned, all prefixes are permitted.

In IPv6 address family mode, the command accepts either an IPv4 or an IPv6 address.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router-af)#neighbor 10.130.14.55 prefix-list test in
```

**neighbor remote-as**

Use the `neighbor remote-as` command to configure a neighbor and identify the neighbor’s autonomous system.

**Syntax**

```
neighbor { ip-address | ipv6-address [interface vlan vlan-id] | autodetect interface interface-id } remote-as as-number

no neighbor { ip-address | ipv6-address [interface vlan vlan-id] | autodetect interface interface-id } remote-as
```

- **ip-address**—The neighbor’s IPv4 address. For external peers, this address must be an IPv4 address on the link that connects the two peers. For internal peers, the neighbor address can be any address, such as the IPv4 address of a loopback interface.

- **ipv6-address**—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. This command is available in IPv6 address family mode.

- **interface vlan vlan-id**—The local routing interface/VLAN ID over which the IPv6 neighbor can be reached. Range: 1-4093.

- **autodetect interface interface-id**—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface. Range is 1–4093.
• remote-as as-number—The autonomous system number of the neighbor’s AS. The range is 1 to 65,535. If the neighbor’s AS number is the same as the local router and the peer is considered an internal peer. Otherwise, the peer is an external peer.

**Default Configuration**

No neighbors are configured by default.

**Command Mode**

BGP Router Configuration mode  
IPv4 Address Family Configuration mode

**User Guidelines**

Up to 100 neighbors can be configured.

**Command History**

Introduced in version 6.2.0.1 firmware.  
Updated in version 6.3.0.1 firmware.

**Example**

```
console(config-router)#neighbor 10.130.14.55 remote-as 10
```

**neighbor remove-private-as**

Use the `neighbor remove-private-as` command to remove private AS numbers when advertising IPv4 routes to an external peer. To stop removing private AS numbers, use the `no` form of this command.

**Syntax**

```
neighbor  { ip-address | ipv6-address [interface vlan vlan-id]} remove-private-as [ all replace-as ]
no neighbor  { ip-address | ipv6-address [interface vlan vlan-id]} remove-private-as
```

• ip-address – The neighbor’s IPv4 address.
• ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
• interface vlan vlan-id—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range 1-4093.
• all replace-as—(Optional) To retain the original AS path length, replace each private AS number with the local AS number.

Default Configuration
Private AS numbers are not removed by default.

Command Mode
BGP Router Configuration mode

User Guidelines
This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-router)#neighbor 10.130.14.55 remove-private-as

neighbor rfc5549-support

Use the neighbor rfc5549-support command to enable advertisement of IPv4 routes over IPv6 next hops selectively to an external BGP IPv6 peer. To disable advertisement of these routes, use the no form of this command.
Syntax

neighbor { ipv6-address | autodetect interface interface-id } rfc5549-support

no neighbor { ipv6-address | autodetect interface interface-id } rfc5549-support

- interface-id—A routing interface identifier (VLAN interface).
- ipv6-address — The neighbor’s IPv6 address.
- autodetect interface interface-id — The routing interface on which the neighbor’s link local IPv6 address is auto detected.

Default Configuration

RFC 5549 support is enabled by default for all neighbors.

Command Mode

BGP Router Configuration mode, IPv4 Address Family Configuration mode

User Guidelines

This command can only be applied to external BGP peers via a single hop. The Next Hop Address advertised for the IPv4 prefixes consists of the link-local IPv6 address and the global IPv6 address (if configured on the interface).

When the Extended Next Hop Encoding capability is not received from a neighbor, Dell EMC Networking does not advertise the RFC 5549 routes to the neighbor. The Dell EMC Networking solution is interoperable with routers that do not support RFC 5549.

Command History

Introduced in version 6.3.0.1 firmware.

Example

The following example results in the connected IPv4 networks 1.1.1.0/24 and 2.2.2.0/24 advertised with next hop set to 2001::1 only to eBGP IPv6 peer 2001::2 and not to eBGP peer 2002::2.

```console
console(config)#ip routing
console(config)#ipv6 unicast-routing
console(config)#vlan 10,20,30
```
console(config-vlan10,20,30)#exit
cfg(config)#interface vlan 10
cfg(config-if-vlan10)#ipv6 enable
cfg(config-if-vlan10)#ipv6 address 2001::1/64
cfg(config-if-vlan10)#exit
cfg(config)#interface vlan 20
cfg(config-if-vlan20)#ipv6 enable
cfg(config-if-vlan20)#ip address 1.1.1.1 /24
cfg(config-if-vlan20)#ipv6 address 2002::1/64
cfg(config-if-vlan20)#exit
cfg(config)#interface vlan 30
cfg(config-if-vlan30)#ip address 2.2.2.2 /24
cfg(config-if-vlan30)#exit
cfg(config)#router bgp 100
cfg(config-router)#redistribute connected
cfg(config-router)#neighbor 2001::2 remote-as 200
cfg(config-router)#neighbor 2001::2 rfc5549-support
cfg(config-router)#neighbor 2002::2 remote-as 300

**neighbor route-map (BGP Router Configuration)**

Use the `neighbor route-map` command to apply a route map to incoming or outgoing routes for a specific neighbor. To remove the route map, use the `no` form of this command.

**Syntax**

```
neighbor ip-address route-map map-name { in | out }
```

```
no neighbor ip-address route-map map-name { in | out }
```

- **ip-address**—The neighbor’s IP address.
- **route-map** map-name—The name of the route map to be used to filter route updates on the specified interface.
- **in | out**—Whether the route map is applied to incoming or outgoing routes.

**Default Configuration**

No route maps are applied by default.
**Command Mode**
A route map can be used to change the local preference, MED, or AS Path of a route. Routes can be selected for filtering or modification using an AS path access list or a prefix list. If a `neighbor route-map` statement refers to a non-existent route map, all routes are denied.

Neighbor route maps configured with this command in router configuration mode are only applied to IPv4 routes.

**User Guidelines**
BGP Router Configuration mode

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config-router)#neighbor 10.130.14.55 route-map test in
```

**neighbor route-map (IPv6 Address Family Configuration)**
In IPv6 address family configuration mode, the `neighbor route-map` command specifies a route map to be applied to inbound or outbound IPv6 routes. To remove the route map, use the `no` form of this command.

**Syntax**
```
neighbor { ip-address | ipv6-address [ interface vlan vlan-id ]} route-map map-name { in | out }

no neighbor { ip-address | ipv6-address [ interface vlan vlan-id]} route-map map-name { in | out }
```
- `ip-address`—The neighbor’s IP address.
- `ipv6-address`—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. Valid in IPv6 address family mode.
- `interface vlan vlan-id`—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range 1-4093.
• route-map map-name—The name of the route map to be used to filter route updates on the specified interface.
• in | out—Whether the route map is applied to incoming or outgoing routes.

Default Configuration
No route maps are applied by default.

Command Mode
IPv6 Address Family Configuration mode

User Guidelines
A route map can be used to change the local preference, MED, or AS Path of a route. Routes can be selected for filtering or modification using an AS path access list or a prefix list. If a neighbor route-map statement refers to a non-existent route map, all routes are denied.

Neighbor route maps configured with this command in router configuration mode are only applied to IPv4 routes. In IPv6 address family mode, the command accepts either an IPv4 or an IPv6 address.

Command History
Introduced in version 6.2.0.1 firmware.

Example
csrole(config-router-af)#neighbor 10.130.14.55 route-map test in

neighbor route-reflector-client (BGP Router Configuration)
To configure an internal peer as an IPv4 route reflector client, use the neighbor route-reflector-client command.

Syntax
neighbor ip-address route-reflector-client
no neighbor ip-address route-reflector-client
• ip-address—The neighbor’s IPv4 address.

**Default Configuration**

Peers are not route reflector clients by default.

**Command Mode**

BGP Router Configuration

**User Guidelines**

Normally, a router does not re-advertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router will re-advertise such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the `bgp cluster-id` command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#neighbor 10.130.14.55 route-reflector-client
```

**neighbor route-reflector-client (IPv6 Address Family Configuration)**

To configure an internal peer as an IPv4 route reflector client, use the `neighbor route-reflector-client` command.
**Syntax**

`neighbor { ip-address | ipv6-address [ interface vlan vlan-id ] } route-reflector-client`

`no neighbor { ip-address | ipv6-address [ interface vlan vlan-id ]} route-reflector-client`

- `ip-address`—The neighbor’s IPv4 address.
- `ipv6-address`—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- `interface vlan vlan-id`—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range 1-4093.

**Default Configuration**

Peers are not route reflector clients by default.

**Command Mode**

IPv6 Address Family Configuration

**User Guidelines**

Normally, a router does not re-advertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router will re-advertise such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the `bgp cluster-id` command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

**Command History**

Introduced in version 6.2.0.1 firmware.
**Example**

```
console(config-router-af)#neighbor 10.130.14.55 route-reflector-client
```

**neighbor send-community (BGP Router Configuration)**

Use the `neighbor send-community` command to configure the local router to send the BGP communities attribute in UPDATE messages to a specific neighbor.

**Syntax**

```
neighbor ip-address send-community
no neighbor ip-address send-community
```

- `ip-address` – The neighbor’s IPv4 address.

**Default Configuration**

The communities attribute is not sent to neighbors by default.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

There are no user guidelines.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-router)#neighbor 10.130.14.55 send-community
```
neighbor send-community (IPv6 Address Family Configuration)

In IPv6 address family configuration mode, the neighbor send-community command tells BGP to send the COMMUNITIES attribute with routes advertised to the peer.

Syntax

neighbor { ip-address | ipv6-address [ interface interface-id ]} send-community

no neighbor { ip-address | ipv6-address [ interface interface-id ]} send-community

- ip-address – The neighbor’s IPv4 address.
- ipv6-address [ interface interface-id ] – The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.

Default Configuration

The communities attribute is not sent to neighbors by default.

Command Mode

IPv6 Address Family Configuration mode

User Guidelines

The command accepts either an IPv4 or an IPv6 address.

Command History

Introduced in version 6.2.0.1 firmware.

Example

cconsole(config-router-af)#neighbor 10.130.14.55 send-community
neighbor shutdown

Use the neighbor shutdown command to administratively disable communications with a specific BGP neighbor. The effect is to gracefully bring down the adjacency with the neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

Syntax

neighbor { ip-address | ipv6-address [interface interface-id] | autodetect interface interface-id } shutdown

no neighbor { ip-address | ipv6-address [interface interface-id] | autodetect interface interface-id } shutdown

- ip-address – The neighbor’s IPv4 address. This is the IP address of the neighbor on the connected link.
- ipv6-address – The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified. Valid in IPv6 address family configuration mode.
- interface-id – The local VLAN routing interface over which the IPv6 neighbor can be reached. Use the vlan keyword and a VLAN ID. Range 1-4093.
- autodetect interface interface-id—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface. Range is 1–4093.

Default Configuration

Neighbors are administratively enabled by default.

Command Mode

BGP Router Configuration, IPv4 Address Family Configuration, IPv6 Address Family Configuration
User Guidelines

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively re-enabled (using no neighbor shutdown).

Command History

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

Example

console(config-router)#neighbor 10.130.14.55 shutdown

neighbor timers

Use the neighbor timers command to override the global keepalive and hold timer values as well as set the keepalive and hold timers for a specific neighbor.

Syntax

neighbor { ip-address | ipv6-address [ interface vlan vlan-id ] | autodetect interface interface-id } timers keepalive holdtime

no neighbor { ip-address | ipv6-address [ interface vlan vlan-id ] | autodetect interface interface-id } timers

- ip-address—The neighbor’s IPv4 address. This is the IP address of the neighbor on the connected link.
- ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- interface vlan vlan-id—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range 1-4093.
- autodetect interface interface-id—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface. Range is 1-4093.
• keepalive—The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. A small internal jitter is applied to the keepalive interval timer in order to reduce the CPU load that may occur when multiple timers expire simultaneously.

• holdtime—The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0, 3 to 65,535 seconds.

Default Configuration
The keepalive and hold timers default to the globally configured values set with the timers bgp command.

Command Mode
BGP Router Configuration mode, IPv4 Address Family Configuration mode

User Guidelines
The new values are not applied to adjacencies already in the ESTABLISHED state. Updated keepalive or hold time values are only applied when an adjacency is newly formed.

Command History
Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

Example
console(config-router)#neighbor 10.130.14.55 timers 1000 500

neighbor update-source
The neighbor update-source command configures BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer BGP router as the neighbor address for this router.
Syntax

neighbor { ip-address | ipv6-address [ interface vlan vlan-id ] | autodetect interface interface-id } } update-source interface

no neighbor { ip-address | ipv6-address [ interface vlan vlan-id ] | autodetect interface interface-id } } update-source

- ip-address—The neighbor’s IPv4 address. This is the IP address of the neighbor on the connected link.
- ipv6-address—The neighbor’s IPv6 address. If the neighbor’s IPv6 address is a link local address, the local interface must also be specified.
- interface vlan vlan-id—The local interface/VLAN ID over which the IPv6 neighbor can be reached. Range: 1-4093.
- autodetect interface interface-id—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface. Range is 1–4093.
- update-source interface—Use the primary IPv4 address on the specified interface as the source IP address for the TCP connection with the neighbor.

Default Configuration

When no update source is configured, the BGP TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Command Mode

BGP Router Configuration mode, IPv4 Address Family Configuration mode

User Guidelines

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor on the peer BGP router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.
It is common to use an IP address on a loopback interface as an update source because a loopback interface is always reachable as long as any routing interface is up. The peering session will stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that interface goes down.

**Command History**

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

**Example**

```
console(config-router)#neighbor 10.130.14.55 update-source 100
```

**network (BGP Router Configuration)**

The `network` command configures BGP to advertise an address prefix. The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

**Syntax**

```
network prefix mask network-mask [ route-map rm-name ]
no network prefix mask network-mask [ route-map rm-name ]
```

```
network ipv6-prefix/prefix-length [ route-map rm-name ]
no network ipv6-prefix/prefix-length
```

- **prefix**—An IPv4 address prefix in dotted decimal notation.
- **network-mask**—The network mask for the prefix in dotted-quad notation (e.g., 255.255.0.0) where a zero bit in the mask indicates a don’t care condition for the corresponding address bits.
- **ipv6-prefix**—An IPv6 network prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons.
- **prefix-length**—The length of the IPv6 prefix given as part of the ipv6-prefix. Required if a prefix is specified. A decimal value in the range 1 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.

- **rm-name**—The name of a route map used to filter prefixes or set attributes of prefixes advertised by this network. The route map statements are evaluated in order, and the first match terminates processing of the route map. If the specified route map does not exist, the network prefix is not advertised (all routes are denied).

### Default Configuration

No networks are advertised by default.

### Command Mode

BGP Router Configuration

### User Guidelines

BGP supports up to 64 networks. The network command may also be used specify a default route (**network 0.0.0.0 mask 0.0.0.0**).

If a route map is configured to set attributes on the advertised routes, **match as-path** and **match community** terms in the route map are ignored. A **match ip-address prefix-list** term is honored in this context. If the route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If the specified route map does not exist, the network is not advertised.

### Command History

Introduced in version 6.2.0.1 firmware.

### Example

```console
console(config-router)#network 10.130.14.55 255.255.0.0
```
network (IPv6 Address Family Configuration)

In IPv6 address family configuration mode, the `network` command identifies network IPv6 prefixes that BGP originates in route advertisements to its neighbors.

**Syntax**

```
network prefix mask network-mask [ route-map rm-name ]
no network prefix mask network-mask [ route-map rm-name ]
network ipv6-prefix/prefix-length [ route-map rm-name ]
no network ipv6-prefix/prefix-length
```

- `prefix`—An IPv4 address prefix in dotted decimal notation.
- `network-mask`—The network mask for the prefix in dotted-quad notation (e.g., 255.255.0.0) where a zero bit in the mask indicates a don’t care condition for the corresponding address bits.
- `ipv6-prefix`—An IPv6 network prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons.
- `prefix-length`—The length of the IPv6 prefix given as part of the `ipv6-prefix`. Required if a prefix is specified. A decimal value in the range 1 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.
- `rm-name`—The name of a route map used to filter prefixes or set attributes of prefixes advertised by this network. The route map statements are evaluated in order, and the first match terminates processing of the route map. If the specified route map does not exist, the network prefix is not advertised (all routes are denied).

**Default Configuration**

No networks are advertised by default.

**Command Mode**

IPv6 Address Family Configuration
User Guidelines

BGP supports up to 64 networks. The network command may also be used to specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, match as-path and match community terms in the route map are ignored. A match ip-address prefix-list term is honored in this context. If the route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If the specified route map does not exist, the network is not advertised.

Example

console(config-router-af)#network 10.130.14.55 255.255.0.0

Default Configuration

The default tag value is 0.

There is no default metric or route map configured.

Command Mode

Router BGP Configuration mode

User Guidelines

The configured metric value is specific to the routes distributed. Use the default-metric command to configure a default metric for all redistributed routes.

The RIP metric is a hop count. The metric for a redistributed route limits the distance the route can be redistributed in the RIP network. Since the maximum valid metric in a RIP network is 15, redistributing routes into RIP with a metric of 12 implies that the route can only be redistributed across 3 hops in the RIP network.

In general, redistributing routes from BGP into a RIP network is not recommended.

Command History

Introduced in version 6.2.0.1 firmware.
Example

console(config-router)#redistribute rip

rd

Use the `rd` command to configure a BGP routing session to advertise VPN-IPv4 prefixes. Use the `no` form of this command to delete the VPN-IPv4 configuration.

Syntax

```
rd route-distinguisher
no rd
```

route-distinguisher— A 2-byte or an 8-byte value to be prepended to an IPv4 prefix to create a VPN IPv4 prefix. The RD value can be specified in either of the following formats:

- 16-bit AS number: a 32-bit value (Ex: 100:11)
- 32-bit IPv4 address: a 16-bit value (Ex: 10.1.1.1:22)

Default Configuration

VRG configuration mode

Command Mode

Privileged Exec mode

User Guidelines

An RD creates routing and forwarding table instance and specifies the default route distinguisher for a VPN. The RD is prepended to IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN related – Composed of an autonomous system number and an arbitrary number.
- IP address related – Composed of an IP address and an arbitrary number.

Once an RD has been configured, it may not be reconfigured. Use the `no` form of the command to remove the RD before configuring a new RD value.
This command is effective only if BGP is running on the router.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
The following example shows how to configure an RD for a VRF instance in ASN format:

```
console(config)#ip vrf Customer_A
console(config-vrf-Customer_A)#rd 62001:10
console(config-vrf-Customer_A)#exit
```

The following example shows how to configure an RD for a VRF instance in IPv4 address format:

```
console(config)#ip vrf Customer_A
console(config-vrf-Customer_A)#rd 192.168.10.1:10
console(config-vrf-Customer_A)#exit
```

**redistribute (BGP)**
The `redistribute` command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, OSPF, and RIP routes.

**Syntax**
```
redistribute { ospf [match { [internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2] } ] | rip | connected | static} [metric metric-value] [route-map map-tag]
```
```
no redistribute { ospf [match { [internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2] } ] | rip | connected | static} [metric metric-value] [route-map map-tag]
```
- **ospf**, **rip**, **connected**, **static**—A source of routes to redistribute.
- **metric** metric-value—(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP (**default metric** command), the MED is set to the default metric. If both a default metric and a metric value are not configured, the prefix is advertised without an MED attribute.
• **match**—(Optional) By default, if BGP is configured to redistribute OSPF routes, BGP only redistributes internal routes (OSPF intra-area and inter-area routes). Use of the **match** option configures BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes. The match option is only valid for OSPF originated routes.

• **route-map map-tag**—(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list.

**Default Configuration**

BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

**Command Mode**

BGP Router Configuration mode

**User Guidelines**

The **distribute-list out** command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

Successful invocations of the **redistribute** command are additive. The **redistribute** command does not overwrite previous **redistribute** command configuration or the default configuration. Use the **no redistribute** command to remove the redistribution of internal or external routes.

A default route cannot be redistributed unless the **default-information-originate** command is given.

The configured metric value is specific to the routes distributed. Use the default-metric command to configure a default metric for all redistributed routes.

The RIP metric is a hop count. The metric for a redistributed route limits the distance the route can be redistributed in the RIP network. Since the maximum valid metric in a RIP network is 15, redistributing routes into RIP with a metric of 12 implies that the route can only be redistributed across 3 hops in the RIP network.
In conformance with RFC 1475, information learned via BGP from peers within the same AS is not redistributed to OSPF.

In general, redistributing routes from BGP into a RIP network is not recommended.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

console(config-router)#redistribute rip

**redistribute (BGP IPv6)**

In IPv6 address family configuration node, the `redistribute` command configures BGP to redistribute non-BGP originated routes from the IPv6 routing table.

**Syntax**

redistribute { ospf [match [{[internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]}] } | rip | connected | static} [metric metric-value] [route-map map-tag]

no redistribute { ospf [match [{[internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]}] } | rip | connected | static} [metric metric-value] [route-map map-tag]

- **ospf, rip, connected, static**—A source of routes to redistribute.
- **metric metric-value**—(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP (default metric command), the MED is set to the default metric. If both a default metric and a metric value are not configured, the prefix is advertised without a MED attribute.
- **match**—(Optional) By default, if BGP is configured to redistribute OSPF routes (redistribute ospf command), BGP only redistributes internal routes (OSPF intra-area and inter-area routes). Use of the match option configures BGP to also redistribute specific types of external or internal routes, or to disable redistribution of OSPF routes. The match option is
only valid for OSPF originated routes. Successive redistribute commands are additive. Use the no form of the command to disable redistribution of a route source.

- **route-map** map-tag—(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list.

**Default Configuration**

BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the match option specifies external routes.

**Command Mode**

IPv6 Address Family Configuration mode

**User Guidelines**

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

Successive invocations of the redistribute command are additive. The redistribute command does not overwrite previous redistribute command configuration or the default configuration. Use the no redistribute command to remove the redistribution of internal or external routes.

A default route cannot be redistributed unless the default-information-originate command is given. The configured metric value is specific to the routes distributed. Use the default-metric command to configure a default metric for all redistributed routes.

In IPv6 address family configuration mode, the syntax and behavior is the same as for IPv4, except that Dell EMC Networking does not support RIP for IPv6.

In conformance with RFC 1475, information learned via BGP from peers within the same AS is not redistributed to OSPF.

**Command History**

Introduced in version 6.2.0.1 firmware.
Example
```
console(config-router-af)#redistribute rip
```

route-target

Use the `route-target` command to create a list of export, import, or both route target (RT) extended communities for the specified VRF instance.

Use the `no` form of the command to remove the route target from a VRF instance.

Syntax

```
route-target {export | import | both} rt-ext-comm
no route-target {export | import | both} rt-ext-comm
```

- `export` — Exports routing information to the target VPN extended community.
- `import` — Imports routing information from the target VPN extended community.
- `both` — Exports and imports the routing information to/from the target VPN extended community.
- `rt-ext-comm` — The route-target extended community attributes to be added to the list of import, export or both (import and export) route-target extended communities.

The route target specifies a target VPN extended community. Like a route distinguisher, the route-target extended community can be specified in either of the following formats:

- 16-bit AS number :your 32-bit value (Ex: 100:11)
- 32-bit IPv4 address :your 16-bit value (Ex: 10.1.1.1:22)

Default Configuration

No route targets are configured by default.

Command Mode

Privileged Exec mode
**User Guidelines**

Configure the route-target command once for each target extended community. Routes that are learned and carry a specific route-target extended community are imported into all VRFs configured with that particular extended community as an import route target.

The configured export RT is advertised as an extended community in the MP-BGP format to the eBGP peer. An RT is either:

- ASN related – Composed of an autonomous system number and an arbitrary number.
- IP address related – Composed of an IP address and an arbitrary number.

This command is effective only if BGP is running on the router.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example shows how to configure route target extended community attributes for a VRF instance in IPv4. The result of this command sequence is that VRF named Customer_A has two export extended communities (100:10 and 300:10) and two import extended communities (300:10 and 192.168.10.1:10).

```
console(config)#ip vrf Customer_A
console(config-vrf-Customer_A)#route-target export 100:10
console(config-vrf-Customer_A)#route-target import 192.168.10.1:10
console(config-vrf-Customer_A)#route-target both 300:10
console(config-vrf-Customer_A)#exit
```

**set extcommunity rt**

Use the `set extcommunity rt` command to set BGP extended community attributes for the route target. Use the `no` form of the command to remove the extended community attributes for the route target.

⚠️ NOTE: This command is effective only if BGP is running on the router.

**Syntax**

```
set extcommunity rt value [additive]
```
no set extcommunity rt

• value — Specifies the route target extended community value. This value can be entered in one of the following formats:
  – 16-bit AS number :your 32-bit value (Ex : 100 :11)
  – 32-bit IPv4 address :your 16-bit value (Ex : 10.1.1.1 :22)
• additive—Adds a route target to the existing route target list without replacing any existing route targets.

Default Configuration
No RT extended community attributes are set.

Command Mode
Route Map Configuration mode

User Guidelines
The route target (RT) extended community attribute is configured with the `rt` keyword. This attribute is used to identify VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. Only one route target can be specified in a single `set extcommunity rt` command. To specify more than one route target, issue the command again with the `additive` keyword.

By default, specifying route targets causes the system to replace existing route targets with the new route targets, unless the `additive` keyword is used. The use of the `additive` keyword causes the system to add the new route targets to the existing route target list, but does not replace any existing route targets.

Command History
Introduced in version 6.3.0.1 firmware.

Example
The following example shows how to set the extended community attribute for route target with route-maps.

(R1)(Config)# ip extcommunity-list 10 permit rt 1:1
set extcommunity soo

Use the `set extcommunity soo` command to set BGP extended community attributes for the site of origin. Use the `no` form of the command to remove the extended community attributes for the site of origin.

⚠️ NOTE: This command is effective only if BGP is running on the router.

**Syntax**

```plaintext
set extcommunity soo value [additive]
no set extcommunity soo
```

- **value** — Specifies the site of origin extended community value. This value can be entered in one of the following formats:
  - 16-bit AS number : your 32-bit value (Ex: 100 :11)
  - 32-bit IPv4 address : your 16-bit value (Ex: 10.1.1.1 :22)
- **additive** — Adds a route target to the existing route target list without replacing any existing route targets.

**Default Configuration**

No site of origin extended community attributes are set.

**Command Mode**

Route Map Configuration mode

**User Guidelines**

The site of origin (SOO) extended communities attribute is configured with the `soo` keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multi-homed. The SOO extended community attribute is
configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multi-homed.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example shows how to set the extended community attribute for site of origin with route-maps on the sending BGP router.

```
(R1)(Config)# ip extcommunity-list 10 permit
(R1)(config)# route-map RECV_IN permit 10
(R1)(config-route-map)# set extcommunity soo 10:10
(R1)(config-route-map)# exit
```

The receiving BGP router will apply the route map with an extended community list in the inward direction.

**show bgp ipv6**

Use this command to display IPv6 routes in the BGP routing table. This command deprecates and replaces the `show ipv6 bgp` command.

**Syntax**

```
show bgp ipv6[ipv6-prefix/prefix-length [ longer-prefixes | shorter-prefixes [ length ] ] | filter-list as-path-list ]
```

- `ipv6-prefix`—An IPv6 network prefix. This argument must be in the form where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons. Limits the output to a specific prefix.
- `prefix-length`—The length of the IPv6 prefix given as part of the ipv6-prefix. This is required if a prefix is specified. A decimal value in the range 1 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.
• **longer-prefixes**—Displays the specified prefix and any longer prefixes within the same range.

• **shorter-prefixes [ length ]**—Used with the ipv6-prefix/prefix-length option to show routes whose prefix length is shorter than prefix-length, and, optionally, longer than a specified length. This option may not be given if the longer-prefixes option is given.

• **filter-list as-path-list**—Filters the output to the set of routes that match the specified AS Path list. This option may not be given if an ipv6-prefix/prefix-length option is given.

**Default Configuration**
There is no default configuration.

**Command Mode**
User Exec mode, Privileged Exec mode, Global Configuration mode and all sub-modes

**User Guidelines**
The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
</tbody>
</table>
| Status codes   | • s—The route is aggregated into an aggregate address configured with the summary-only option  
|                 | • *—Dell EMC Networking BGP never displays invalid routes; so this code is always displayed (to maintain consistency with the industry standard)  
|                 | • >—Indicates that BGP has selected this path as the best path to the destination  
|                 | • i—If the route is learned from an internal peer                          |
| Network        | IPv6 Destination prefix                                                      |
| Next Hop       | The route’s BGP next hop                                                    |
| Metric         | Multi-Exit Discriminator                                                    |
Layer 3 Routing Commands

Command History
Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

Example

```console
console# show bgp ipv6
BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2001:DB8::/48</td>
<td>3FFE:100::1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
<tr>
<td></td>
<td>3FFE:200::4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*&gt; 2001:DB8:4:5::/64</td>
<td>3FFE:100::1</td>
<td>10</td>
<td>100</td>
<td>20 10 ?</td>
</tr>
</tbody>
</table>
```

**show bgp ipv6 aggregate-address**

Use this command to display the configured IPv6 aggregate addresses and indicates if each address is currently active. This command replaces and deprecates the `show ipv6 bgp aggregate-address` command.

**Syntax**

```
show bgp ipv6 aggregate address-group
```

**Default Configuration**

There is no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocPrf</td>
<td>The local preference</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path</td>
</tr>
<tr>
<td>Origin</td>
<td>The value of the Origin attribute</td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

Command History
Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

Example

console# show bgp ipv6 aggregate-address

<table>
<thead>
<tr>
<th>Prefix/Len</th>
<th>AS Set</th>
<th>Summary Only</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8::/48</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>3ffe:4000:1::/48</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

show bgp ipv6 community

Use this command to display IPv6 routes that belong to the specified set of communities. This command replaces and deprecates the `show ipv6 bgp community` command.

Syntax

show bgp ipv6 community communities [ exact-match ]

- communities—A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
- exact-match—Only displays routes that are members of those and only those communities specified in the command.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**
The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
</tbody>
</table>
| Status codes   | • s—The route is aggregated into an aggregate address configured with the summary-only option  
                • °—Dell EMC Networking BGP never displays invalid routes; so this code is always displayed (to maintain consistency with the industry standard)  
                • >—Indicates that BGP has selected this path as the best path to the destination  
                • i—If the route is learned from an internal peer |
| Network        | IPv6 Destination prefix                                                     |
| Next Hop       | The route’s BGP next hop                                                    |
| Metric         | Multi-Exit Discriminator                                                    |
| LocPrf         | The local preference                                                        |
| Path           | The AS path                                                                 |

**Command History**
Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

**Example**

```
console(config)#show bgp ipv6 community
```
show bgp ipv6 community-list

Use this command to display the IPv6 routes that match a specified community list.

Syntax

show bgp ipv6 community-list name [ exact-match ]
  • name—A standard community list name.
  • exact-match—Displays only routes that are an exact match for the set of communities in the matching community list statement.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

User Guidelines

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
</tbody>
</table>
Command History

Introduced in version 6.2.0.1 firmware.

Example

BGP table version is 0, local router ID is 65.1.1.1
Status Codes: s suppressed, * valid, > best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network IPv6 Destination prefix</th>
<th>Next Hop The route’s BGP next hop</th>
<th>Metric Multi-Exit Discriminator</th>
<th>LocPrf The local preference</th>
<th>Path The AS path</th>
</tr>
</thead>
</table>

show bgp ipv6 listen range

Use the show bgp ipv6 listen range command to display information about IPv6 BGP listen ranges.

Syntax

show bgp ipv6 [vrf vrf-name] listen range [ network/length ]

- network/length — Displays information about the specified listen range.
- vrf-name—The name of a previously configured VRF.
**Default Configuration**
There is no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
There are no usage guidelines.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**

```
console#show bgp ipv6 listen range

Listen Range.................................. 2001::1/64
Inherited Template............................ template_2001

<table>
<thead>
<tr>
<th>Member</th>
<th>ASN</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::10</td>
<td>65001</td>
<td>OPENCONFIRM</td>
</tr>
<tr>
<td>2001::20</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Listen Range.................................. 2002::1/64
Inherited Template............................ template_2002

show bgp ipv6 neighbors
```

Use this command to display neighbors with IPv4 or IPv6 peer addresses that are enabled for the exchange of IPv6 prefixes. This command deprecates and replaces the `show ipv6 bgp neighbors` command.

**Syntax**

```
show bgp ipv6 neighbors [ ipv4-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id ]
```
• **ipv4-address | ipv6-address**—(Optional) If a peer address is specified, the output is limited to an individual peer.

• **interface-id**—(Optional) If the peer address is an IPv6 link local address, the interface that defines the scope of the link local address must be given. This must be a VLAN routing interface.

• **autodetect interface interface-id**—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**

• “RFC 5549 Support” is displayed only if the BGP neighbor is peered over IPv6 network.

• If the peer is configured as “autodetect”, the “Remote Address” shows detected IPv6 address or “Unresolved” in case if the peer is not detected by the autodetect feature.

• “Autodetect status” is displayed only if the peer is configured as “autodetect”. The field shows one of the following statuses:
  • Peer is detected
  • Peer is not detected
  • Multiple peers are detected

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>The neighbor’s IPv6 address. If this is a link local address, the next line indicates the scope of the address.</td>
</tr>
<tr>
<td>Remote AS</td>
<td>The neighbor’s autonomous system number</td>
</tr>
<tr>
<td>Peer ID</td>
<td>The neighbor’s BGP router ID</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Peer Admin Status</td>
<td>START or STOP</td>
</tr>
<tr>
<td>Peer State</td>
<td>The adjacency state of this neighbor</td>
</tr>
<tr>
<td>Peer Type</td>
<td>The type of peer</td>
</tr>
<tr>
<td>Listen Range</td>
<td>The ports that are being listened to.</td>
</tr>
<tr>
<td>Local Port</td>
<td>TCP port number on the local end of the connection</td>
</tr>
<tr>
<td>Remote Port</td>
<td>TCP port number on the remote end of the connection</td>
</tr>
<tr>
<td>Connection Retry Interval</td>
<td>How long BGP waits between connection retries</td>
</tr>
<tr>
<td>Neighbor Capabilities</td>
<td>Optional capabilities reported by the neighbor, recognized and accepted by this router. Codes listed in the show output are as follows:</td>
</tr>
<tr>
<td></td>
<td>• MP: Multiprotocol</td>
</tr>
<tr>
<td></td>
<td>• RF: Route Refresh</td>
</tr>
<tr>
<td></td>
<td>This version of Dell EMC Networking does not support any multiprotocol AFI/SAFI pairs other than IPv4 unicast. The presence of this capability does not imply otherwise.</td>
</tr>
<tr>
<td>IPv4 Unicast Support</td>
<td>Indicates whether IPv4 unicast routes can be exchanged with this peer. Both indicates that IPv4 is active locally and the neighbor indicated support for IPv4 unicast in its OPEN message. Sent indicates that IPv4 unicast is active locally, but the neighbor did not include this AFI/SAFI pair in its OPEN message. IPv4 unicast is always enabled locally and cannot be disabled.</td>
</tr>
<tr>
<td>IPv6 Unicast Support</td>
<td>Indicates whether IPv6 unicast routes can be exchanged with this peer. Both and Sent have the same meaning as for IPv4. None indicates that neither the local router nor the peer has IPv6 enabled for this adjacency. Received indicates that the peer advertised the IPv6 unicast capability, but it is not enabled locally. IPv6 unicast is enabled locally using the neighbor activate command in address-family IPv6 configuration mode.</td>
</tr>
<tr>
<td>RFC 5549 Support</td>
<td>If support for RFC 5549 is enabled.</td>
</tr>
<tr>
<td>Update Source</td>
<td>The configured value for the source IP address of packets sent to this peer. This field is only included in the output if the update source is configured.</td>
</tr>
<tr>
<td><strong>Local Interface Address</strong></td>
<td>The IPv6 address used as the source IP address in packets sent to this neighbor.</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Configured Hold Time</strong></td>
<td>The time, in seconds, that this router proposes to this neighbor as the hold time</td>
</tr>
<tr>
<td><strong>Configured Keep Alive Time</strong></td>
<td>The configured KEEPALIVE interval for this neighbor.</td>
</tr>
<tr>
<td><strong>Negotiated Hold Time</strong></td>
<td>The minimum configured hold time and the hold time in the OPEN message received from this neighbor. If the local router does not receive a KEEPALIVE or UPDATE message from this neighbor within this interval of time, the local router drops the adjacency. This field is only shown if the adjacency state is OPEN CONFIRM or greater.</td>
</tr>
<tr>
<td><strong>Keep Alive Time</strong></td>
<td>The number of seconds between KEEPALIVE messages sent to this neighbor. This field is only shown if the adjacency state is OPEN CONFIRM or greater.</td>
</tr>
<tr>
<td><strong>Prefix Limit</strong></td>
<td>The maximum number of prefixes this router is willing to accept from this neighbor.</td>
</tr>
<tr>
<td><strong>Prefix Warning Threshold</strong></td>
<td>Percentage of the prefix limit that causes a warning message to be logged.</td>
</tr>
<tr>
<td><strong>Warning Only on Prefix Limit</strong></td>
<td>Whether to shutdown a neighbor that exceeds the prefix limit. TRUE if the event is logged without shutting down the neighbor.</td>
</tr>
<tr>
<td><strong>Minimum Advertisement Interval</strong></td>
<td>The minimum time between UPDATE messages sent to this neighbor.</td>
</tr>
<tr>
<td><strong>MD5 Password</strong></td>
<td>The TCP MD5 password, if one is configured, in plain text.</td>
</tr>
<tr>
<td><strong>Last Error</strong></td>
<td>The last error that occurred on the connection to this neighbor.</td>
</tr>
<tr>
<td><strong>Last SubError</strong></td>
<td>The suberror reported with the last error.</td>
</tr>
<tr>
<td><strong>Time Since Last Error</strong></td>
<td>How long since an error has occurred.</td>
</tr>
<tr>
<td><strong>Established Transitions</strong></td>
<td>The number of times the adjacency has transitioned into the Established state.</td>
</tr>
<tr>
<td><strong>Established Time</strong></td>
<td>How long since the connection last transitioned to or from the Established state.</td>
</tr>
<tr>
<td><strong>Time Elapsed Since Last Update</strong></td>
<td>How long since an UPDATE message has been received from this neighbor.</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>IPv6 Outbound Update Group</strong></td>
<td>The IPv6 outbound update group.</td>
</tr>
<tr>
<td><strong>Message Table</strong></td>
<td>The number of BGP messages sent to and received from this neighbor.</td>
</tr>
<tr>
<td><strong>Received Update Queue Size</strong></td>
<td>Received UPDATE messages are queued for processing. This section shows the current length of the neighbor’s UPDATE queue in bytes, the high water mark, the limit, and the number of UPDATEs that have been dropped because the queue reached the limit.</td>
</tr>
</tbody>
</table>

The following fields are displayed for IPv4 and for IPv6.

<table>
<thead>
<tr>
<th><strong>Prefixes Advertised</strong></th>
<th>A running count of the number of prefixes advertised to or received from this neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PrefixesWithdrawn</strong></td>
<td>A running count of the number of prefixes included in the Withdrawn Routes portion of UPDATE messages, to and from this neighbor.</td>
</tr>
<tr>
<td><strong>Prefixes Current</strong></td>
<td>The number of prefixes currently advertised to or received from this neighbor. For inbound prefixes, this count only includes prefixes that passed inbound policy.</td>
</tr>
<tr>
<td><strong>Prefixes Accepted</strong></td>
<td>The number of prefixes from this neighbor that are eligible to become active in the local RIB. Received prefixes are ineligible if their BGP Next Hop is not resolvable or if the AS Path contains a loop. A prefix is only considered accepted if it passes inbound policy.</td>
</tr>
<tr>
<td><strong>Prefixes Rejected</strong></td>
<td>The number of prefixes currently received from this neighbor that fail inbound policy.</td>
</tr>
<tr>
<td><strong>Max NLFI per Update</strong></td>
<td>The maximum number of prefixes included in a single UPDATE message, to and from this neighbor.</td>
</tr>
<tr>
<td><strong>Min NLRI per Update</strong></td>
<td>The minimum number of prefixes included in a single UPDATE message, to and from this neighbor.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware. Modified in version 6.3.0.1 firmware.
Example

console# show bgp ipv6 neighbors fe80::2

Description: spine 1 router 1

Remote Address.............................. fe80::2
Interface..................................... 0/1
Remote AS..................................... 100
Peer ID....................................... 14.3.0.1
Peer Admin Status............................ START
Peer State.................................... ESTABLISHED
Peer Type.................................... DYNAMIC
Local Port.................................... 179
Remote Port................................... 58265
Connection Retry Interval..................... 120 sec
Neighbor Capabilities........................ None
IPV4 Unicast Support........................ None
IPV6 Unicast Support........................ Both
RFC 5549 Support.............................. Enable
Update Source.................................. None
Local Interface Address....................... fe80::2
Configured Hold Time......................... 90 sec
Configured Keep Alive Time................... 30 sec
Negotiated Hold Time......................... 30 sec
Keep Alive Time.............................. 10 sec
MD5 Password................................ password

Last Error (Sent).............................. Hold Timer Expired
Last SubError................................ None
Time Since Last Error........................ 0 day 0 hr 4 min 27 sec
Established Transitions...................... 1
Established Time.............................. 0 day 0 hr 4 min 25 sec
Time Since Last Update....................... 0 day 0 hr 4 min 24 sec
IPv6 Outbound Update Group................... 7

<table>
<thead>
<tr>
<th>Open</th>
<th>Update</th>
<th>Keepalive</th>
<th>Notification</th>
<th>Refresh</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msgs Sent</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>Msgs Rcvd</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

Received UPDATE Queue Size: 0 bytes. High: 355. Limit 196096. Drops 0.

IPv6 Prefix Statistics:

<table>
<thead>
<tr>
<th>Prefixes Advertised</th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes Withdrawn</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Current</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Accepted1 N/A</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Prefixes Rejected</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Max NLRI per Update</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Min NLRI per Update</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
show bgp ipv6 neighbors advertised-routes

Use this command to display IPv6 routes advertised to a specific neighbor. The format and field descriptions are the same as for `show ip bgp neighbors advertised-routes`, except that the Network and Next Hop fields show IPv6 addresses. This command deprecates and replaces the `show ipv6 bgp neighbors advertised-routes` command.

**Syntax**

```
show bgp ipv6 neighbors { ipv4-address | ipv6-address [ interface interface-id ] } advertised-routes
```

- `ipv4-address`—The IPv4 address of a BGP peer.
- `ipv6-address [ interface interface-id ]`—The IPv6 address of a BGP peer. If the peer address is an IPv6 link local address, the interface that defines the scope of the link local address must be given.
- `autodetect interface interface-id`—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface ID must be a VLAN routing interface.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
<tr>
<td>Local router ID</td>
<td>The IP address of the local router.</td>
</tr>
</tbody>
</table>
**Status Codes**

- **p** – The route has been updated in Adj-RIB-Out since the last UPDATE message was sent. Transmission of an UPDATE message is pending.

**Network**

The Destination prefix.

**Next Hop**

The BGP Next Hop as advertised to the peer.

**Metric**

The value of the Multi Exit Discriminator (MED), if the MED is advertised to the peer.

**LocPref**

The local preference. Local preference is never advertised to external peers.

**Path**

The AS path. The AS path does not include the local AS number, which is added to the beginning of the AS path when a route is advertised to an external peer.

**Origin**

The value of the origin attribute.

- **i**—IGP
- **e**—EGP
- **?**—Incomplete

---

**Command History**

Introduced in version 6.2.0.1 firmware.

Modified in version 6.3.0.1 firmware.

---

**Example**

```console
console#show bgp ipv6 neighbors fe80::211:12ff:fe06:4 interface vl10 advertised-routes

BGP table version is 10, local router ID is 0.0.0.100
Status codes: p - advertisement pending
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010:10::/64</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>2020:20::/64</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td>i</td>
</tr>
</tbody>
</table>
```

---
show bgp ipv6 neighbors policy

Use this command to display the inbound and outbound IPv6 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template. This command deprecates and replaces the show ipv6 bgp neighbors policy command.

Syntax

show bgp ipv6 neighbors [ipv4-address | ipv6-address [interface interface-id]] policy

- ipv4-address—The IPv4 address of a neighbor may optionally be specified to limit the output to a single neighbor.
- ipv6-address [interface interface-id]—The IPv6 address of a neighbor. If specified, the output shows only this neighbor. If the neighbor’s address is a link local address, the interface must be specified.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

User Guidelines

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>The peer address of a neighbor.</td>
</tr>
<tr>
<td>Policy</td>
<td>A neighbor-specific BGP policy.</td>
</tr>
<tr>
<td>Template</td>
<td>If the policy is inherited from a peer template, this field lists the template name.</td>
</tr>
</tbody>
</table>

Command History

Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

**Example**

```
console#show bgp ipv6 neighbors fe80::1 vlan 10 policy
```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Policy</th>
<th>Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::1%Vl0010</td>
<td>activate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-list jupiter in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-list saturn out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>maximum-prefix 2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>send-community</td>
<td></td>
</tr>
</tbody>
</table>

**show bgp ipv6 neighbors received-routes**

Use this command to display a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for `show IP bgp neighbors received-routes`, except that they list IPv6 routes. Also, the command displays a list of IPv4 routes received from a specific neighbor with RFC5549.

This command deprecates and replaces the `show ipv6 bgp neighbors received-routes` command.

**Syntax**

```
show bgp ipv6 neighbors { ipv4-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id } { received-routes | routes | rejected-routes }
```

- `ipv4-address`—The IPv4 address of a BGP peer
- `ipv6-address interface interface-id`—The IPv6 address of a BGP peer. If the peer address is an IPv6 link local address, the interface that defines the scope of the link local address must be given.
- `autodetect interface interface-id`—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface.
Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec and all show modes

User Guidelines
The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>The destination prefix.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The BGP Next Hop as advertised by the peer.</td>
</tr>
<tr>
<td>Metric</td>
<td>The value of the MED, if a MED is received from the peer.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The local preference received from the peer.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path as received from the peer.</td>
</tr>
<tr>
<td>Origin</td>
<td>The value of the Origin attribute as received from the peer.</td>
</tr>
</tbody>
</table>

Command History
Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

Example
```
console#show bgp ipv6 neighbors 1010:10::103 routes

Local router ID is 0.0.0.101
Origin codes: i - IGP, e - EGP, ? - incomplete

Network             Next Hop         Metric     LocPref Path     Origin
------------------- ---------------- ---------- ------- ------------- -----
1010:10::/64        1010:10::103     0          65001             i
2020:20::/64        1010:10::103     0          65001             i

console#show bgp ipv6 neighbors fe80::21e:c9ff:fede:b51a interface vlan 10 received-routes

Local router ID is 0.0.0.101
```
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010:10::/64</td>
<td>1010:10::103</td>
<td>0</td>
<td></td>
<td>65001</td>
<td>i</td>
</tr>
<tr>
<td>2020:20::/64</td>
<td>1010:10::103</td>
<td>0</td>
<td></td>
<td>65001</td>
<td>i</td>
</tr>
</tbody>
</table>

**show bgp ipv6 statistics**

Use this command to display statistics for the IPv6 decision process. This command deprecates and replaces the `show ipv6 bgp statistics` command.

**Syntax**

show bgp ipv6 statistics

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration sub-modes.

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>How long since the decision process was run. hours:minutes:seconds if the elapsed time is less than 24 hours. Otherwise, days:hours.</td>
</tr>
<tr>
<td>Phase</td>
<td>The phase of the decision process that was run.</td>
</tr>
<tr>
<td>Upd Grp</td>
<td>Outbound update group ID. Only applies when phase 3 is run.</td>
</tr>
<tr>
<td>GenId</td>
<td>Generation ID of BGP routing table when decision process was run. The generation ID is incremented each time phase 2 of the decision process is run and when there is a change to the status of aggregate addresses.</td>
</tr>
<tr>
<td>Reason</td>
<td>The event that triggered the decision process to run</td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

<table>
<thead>
<tr>
<th>Peer</th>
<th>Phase 1 of the decision process can be triggered for a specific peer when a peer’s inbound routing policy changes or the peer is reset. When phase 1 is run for a single peer, the peer’s IP address is given.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>How long the decision process took, in milliseconds</td>
</tr>
<tr>
<td>Adds</td>
<td>The number of routes added. For phase 1, this is the number of prefixes that pass inbound policy and are added to the Accept-RIB-In. For phase 2, this is the number of routes added to the BGP routing table. For phase 3, this is the number of prefixes added to the update group’s Adj-RIB-Out.</td>
</tr>
<tr>
<td>Mods</td>
<td>The number of routes modified. Always 0 for phase 1</td>
</tr>
<tr>
<td>Dels</td>
<td>The number of routes deleted. Always 0 for phase 1</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

Modified in version 6.3.0.1 firmware.

**Example**

```
console # show bgp ipv6 statistics
```

<table>
<thead>
<tr>
<th>Delta T</th>
<th>Phase</th>
<th>Upd Grp</th>
<th>GenId</th>
<th>Reason</th>
<th>Peer</th>
<th>Duration</th>
<th>Adds</th>
<th>Mods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29:33:49</td>
<td>3</td>
<td>0</td>
<td>2041</td>
<td>Fwd status chng</td>
<td>34</td>
<td>750</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>29:33:40</td>
<td>2</td>
<td></td>
<td>2042</td>
<td>Accept-RIB-In-</td>
<td>59</td>
<td>750</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>29:33:28</td>
<td>2</td>
<td></td>
<td>2043</td>
<td>Accept-RIB-In-</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>250</td>
</tr>
<tr>
<td>29:23:40</td>
<td>2</td>
<td></td>
<td>2044</td>
<td>Accept-RIB-In-</td>
<td>32</td>
<td>0</td>
<td>0</td>
<td>1000</td>
</tr>
<tr>
<td>29:13:40</td>
<td>3</td>
<td>1</td>
<td>2044</td>
<td>Phase 2 done</td>
<td>48</td>
<td>500</td>
<td>2500</td>
<td>1750</td>
</tr>
<tr>
<td>29:02:01</td>
<td>3</td>
<td>0</td>
<td>2044</td>
<td>Phase 2 done</td>
<td>41</td>
<td>750</td>
<td>0</td>
<td>1250</td>
</tr>
<tr>
<td>28:33:40</td>
<td>2</td>
<td></td>
<td>2045</td>
<td>Phase 1 done</td>
<td>32</td>
<td>500</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28:14:40</td>
<td>2</td>
<td></td>
<td>2046</td>
<td>Phase 1 done</td>
<td>16</td>
<td>250</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**show bgp ipv6 summary**

Use this command to display a summary of BGP configuration and status. This command deprecates and replaces the `show ipv6 bgp summary` command.

**Syntax**

```
show bgp ipv6 summary
```
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration sub-modes.

**User Guidelines**
The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>Whether BGP is globally enabled.</td>
</tr>
<tr>
<td>BGP Router ID</td>
<td>The configured router ID.</td>
</tr>
<tr>
<td>Local AS Number</td>
<td>The router’s AS number.</td>
</tr>
<tr>
<td>Traps</td>
<td>Whether BGP traps are enabled.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an external BGP route.</td>
</tr>
<tr>
<td>Maximum Paths iBGP</td>
<td>The maximum number of next hops in an internal BGP route.</td>
</tr>
<tr>
<td>Default Keep Alive Time</td>
<td>The configured keepalive time used by all peers that have not been configured with a peer-specific keepalive time.</td>
</tr>
<tr>
<td>Default Hold Time</td>
<td>The configured hold time used by all peers that have not been configured with a peer-specific hold time.</td>
</tr>
<tr>
<td>Number of Network Entries</td>
<td>The number of distinct IPv6 prefixes in the local RIB.</td>
</tr>
<tr>
<td>Number of AS Paths</td>
<td>The number of IPv6 AS paths in the local RIB.</td>
</tr>
<tr>
<td>Dynamic Neighbors</td>
<td>The number of dynamically discovered neighbors (current number, maximum number discovered, upper limit allowed).</td>
</tr>
<tr>
<td>Default Metric</td>
<td>The default value for the MED for redistributed routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether BGP is configured to advertise a default route.</td>
</tr>
<tr>
<td>Redistributing</td>
<td>Corresponds to default-information originate.</td>
</tr>
</tbody>
</table>
Source | A source of routes that BGP is configured to redistribute.
--- | ---
Metric | The metric configured with the redistribute command.
Match Value | For routes redistributed from OSPF, the types of OSPF routes being redistributed.
Distribute List | The name of the prefix list used to filter redistributed routes, if one is configured with the `distribute-list out` command.
Route Map | The name of the route map used to filter redistributed routes.
Neighbor | The IP address of a neighbor
ASN | The neighbor’s ASN
MsgRxvd | The number of BGP messages received from this neighbor
MsgSent | The number of BGP messages sent to this neighbor
State | The adjacency state. One of IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST
Up/Down Time | How long the adjacency has been in the ESTABLISHED state, or, if the adjacency is down, how long it has been down. In days:hours:minutes:seconds
Pfx Rcvd | The number of IPv6 prefixes received from the neighbor

**Command History**

Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

**Example**

```console
console#show bgp ipv6 summary
IPv6 Routing ................................. Enable
BGP Admin Mode ................................. Enable
BGP Router ID ................................. 1.1.1.1
Local AS Number ............................. 65001
Traps ........................................... Disable
Maximum Paths ............................... 1
Maximum Paths iBGP .......................... 1
Default Keep Alive Time ..................... 30
```
Default Hold Time ............................. 90
Number of Network Entries ..................... 0
Number of AS Paths ............................ 0
Dynamic Neighbors Current/High/Limit ......... 1/1/20
Default Metric ................................. Not Configured
Default Route Advertise ....................... No

Redistributing:
Source    Metric     Dist List                        Route Map
--------- ---------- -------------------------------- ----------------------

Neighbor         ASN   MsgRcvd  MsgSent  State         Up/Down Time   Pfx Rcvd
---------------- ----- -------- -------- ------------- -------------- ------
fe80::21e:c9ff:fede:b13a%Vl10
65000 137      136      ESTABLISHED                  0

**show bgp ipv6 update-group**

Use this command to report the status of IPv6 outbound groups and their members. Output and format are the same as for `show ip bgp update-group`. This command deprecates and replaces the `show ipv6 bgp update-group` command.

**Syntax**

`show bgp ipv6 update-group [ group-index | ipv4-address | ipv6-address [ interface interface-id ] | autodetect interface interface-id ]`

- **group-index**—If specified, this option restricts the output to a single update group.
- **ipv4-address**—The IPv4 address of a peer enabled for exchange of IPv6 prefixes. If specified, this option restricts the output to the update group containing the peer with the given address.
- **ipv6-address [ interface interface-id ]**—The IPv6 address of a peer. If the peer address is a link local address, the interface that defines the scope of the address must also be given. If a peer address is specified, this option restricts the output to the update group containing the peer with the given address.
- **autodetect interface interface-id**—(Optional) The routing interface on which the neighbor’s link local IPv6 address is auto detected. The interface-id must be a VLAN routing interface.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**
The update send history table show statistics on as many as the fifteen most recent executions of the update send process for the update group. Items in the history table are as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The update version.</td>
</tr>
<tr>
<td>Delta T</td>
<td>The amount of time elapsed since the update send process executed. hours::minutes::seconds.</td>
</tr>
<tr>
<td>Duration</td>
<td>How long the update send process took, in milliseconds</td>
</tr>
<tr>
<td>UPD Built</td>
<td>The number of UPDATE messages built.</td>
</tr>
<tr>
<td>UPD Sent</td>
<td>The number of UPDATE messages successfully transmitted to group members. Normally a copy of each UPDATE message built is sent to each group member.</td>
</tr>
<tr>
<td>Paths Sent</td>
<td>The number of paths advertised.</td>
</tr>
<tr>
<td>Pfxs Adv</td>
<td>The number of prefixes advertised.</td>
</tr>
<tr>
<td>Pfxs Wd</td>
<td>The number of prefixes withdrawn.</td>
</tr>
</tbody>
</table>

The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Group ID</td>
<td>Unique identifier for outbound update group.</td>
</tr>
<tr>
<td>Peer Type</td>
<td>Whether peers in this update group are internal or external.</td>
</tr>
<tr>
<td>Minimum Advertisement Interval</td>
<td>The minimum time, in seconds, between sets of UPDATE messages sent to the group.</td>
</tr>
<tr>
<td><strong>Send Community</strong></td>
<td>Whether BGP communities are included in route advertisements to members of the group. Yes or No.</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Neighbor AS Path Access List Out</strong></td>
<td>The AS path access list used to filter UPDATE messages sent to peers in the update group.</td>
</tr>
<tr>
<td><strong>Neighbor Prefix List Out</strong></td>
<td>Name of the prefix list used to filter prefixes advertised to the peers in the update group.</td>
</tr>
<tr>
<td><strong>Neighbor Route Map Out</strong></td>
<td>Name of the route map used to filter and modify routes advertised to the peers in the update group.</td>
</tr>
<tr>
<td><strong>Members Added</strong></td>
<td>The number of peers added to the group since the group was formed.</td>
</tr>
<tr>
<td><strong>Members Removed</strong></td>
<td>The number of peers removed from the group.</td>
</tr>
<tr>
<td><strong>Update Version</strong></td>
<td>The number of times phase 3 of the BGP decision process has run for this group to determine which routes should be advertised to the group.</td>
</tr>
<tr>
<td><strong>Number of UPDATEs Sent</strong></td>
<td>The number of UPDATE messages that have been sent to this group. Incremented once for each UPDATE regardless of the number of group members.</td>
</tr>
<tr>
<td><strong>Time Since Last UPDATE</strong></td>
<td>Time since an UPDATE message was last sent to the group. If no UPDATE has been sent to the group, the status is “Never.”</td>
</tr>
<tr>
<td><strong>Current Prefixes</strong></td>
<td>The number of prefixes currently advertised to the group.</td>
</tr>
<tr>
<td><strong>Current Paths</strong></td>
<td>The number of paths currently advertised to the group.</td>
</tr>
<tr>
<td><strong>Prefixes Advertised</strong></td>
<td>The total number of prefixes advertised to the group since the group was formed.</td>
</tr>
<tr>
<td><strong>Prefixes Withdrawn</strong></td>
<td>The total number of prefixes included in the Withdrawn Routes field of UPDATE messages sent to the group since the group was formed.</td>
</tr>
<tr>
<td><strong>UPDATE Send Failures</strong></td>
<td>The number of UPDATE messages that failed to be delivered to all members of the group.</td>
</tr>
<tr>
<td><strong>Current Members</strong></td>
<td>The IPv4 address of all current members of the group.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.
show bgp ipv6 route-reflection

Use this command to display a summary of BGP route reflection. This command deprecates and replaces the show ipv6 bgp route-reflection command.

Syntax
show bgp ipv6 route-reflection

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
If a route reflector client is configured with an outbound route map, the output warns that set statements in the route map are ignored when reflecting routes to this client.

The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>The cluster ID used by this router. The value is tagged as configured when the value is configured with the bgp cluster-id command. When no cluster ID is configured, the local router ID is shown and tagged as default.</td>
</tr>
<tr>
<td>Client-to-Client Reflection</td>
<td>Displayed as Enabled when this router reflects routes received from its clients to its other clients. Disabled otherwise.</td>
</tr>
<tr>
<td>Clients</td>
<td>A list of this router’s internal peers which have been configured as route reflector clients.</td>
</tr>
</tbody>
</table>
Non-client Internal Peers | A list of this router’s internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

**Command History**

Introduced in version 6.2.0.1 firmware.
Modified in version 6.3.0.1 firmware.

**Example**

```
console(config)#show bgp ipv6 route-reflection

Cluster ID .................................... 65.1.1.1 (default)
Client-to-client Reflection ................... Enabled
Clients:
Non-client Internal Peers:
```

**show ip bgp**

To view routes in the BGP routing table, use the `show ip bgp` command. The output lists both the best and non-best paths to each destination.

**Syntax**

```
show ip bgp [network/pfx-length [longer-prefixes | shorter-prefixes [length]]] | [filter-list as-path-list ] | [prefix-list list-name]
```

- *network/pfx-length*—(Optional) Display a specific route identified by its destination prefix
- *longer-prefixes*—(Optional) Used with the network/pfx-len option to show routes whose prefix length is equal to or longer than pfx-len. This option may not be given if the *shorter-prefixes* option is given.
- *shorter-prefixes* [ length ]—(Optional) Used with the network/pfx-len option to show routes whose prefix length is shorter than pfx-len, and, optionally, longer than a specified length. This option may not be given if the *longer-prefixes* option is given.
- *filter-list as-path-list*—(Optional) Filter the output to the set of routes that match a given AS Path list. This option may not be given if a network/pfx-len option is given.
• **Prefix-list** list-name — (Optional) The name of a prefix list indicating the list of matching routes to display.

### Default Configuration

There is no default configuration.

### Command Mode

User Exec mode, Privileged Exec mode, Global Configuration mode and all sub-modes.

### User Guidelines

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
</tbody>
</table>
| Status codes        | • s—The route is aggregated into an aggregate address configured with the summary-only option  
                      • *—Dell EMC Networking BGP never displays invalid routes; so this code is always displayed (to maintain consistency with the industry standard)  
                      • >—Indicates that BGP has selected this path as the best path to the destination  
                      • i—If the route is learned from an internal peer |
| Network             | Destination prefix                                                          |
| Next Hop            | The route’s BGP next hop                                                    |
| Metric              | Multi-Exit Discriminator                                                    |
| LocPrf              | The local preference                                                        |
| Path                | The AS path                                                                 |
| Origin              | The value of the Origin attribute                                           |

### Command History

Introduced in version 6.2.0.1 firmware.
**Example**

console# show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 172.20.1.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>200.10.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*&gt; 172.20.2.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

**show ip bgp aggregate-address**

Use the `show ip bgp aggregate-address` command to list the aggregate addresses that have been configured and indicates whether each is currently active.

**Syntax**

```text
show ip bgp [vrf vrf-name] aggregate-address
```

- `vrf vrf-name` — Displays the aggregate address information associated with the named VRF.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

Privileged Exec mode, Global Configuration mode, and all sub-modes.

**User Guidelines**

If the `vrf` argument is specified, information pertaining to that VRF is displayed.

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix/Len</td>
<td>Destination prefix and length</td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

<table>
<thead>
<tr>
<th>AS Set</th>
<th>Indicates whether an empty AS path is advertised with the aggregate address (N) or an AS SET is advertised with the set of AS numbers for the paths contributing to the aggregate (Y).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary Only</td>
<td>Indicates whether the individual networks are suppressed (Y) or advertised (N).</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether the aggregate is currently being advertised.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware. Updated in 6.3.0.1 firmware.

**Example**

```console
console#show ip bgp aggregate-address
```

<table>
<thead>
<tr>
<th>Prefix/Len</th>
<th>AS Set</th>
<th>Summary Only</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.0/24</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>10.10.10.0/24</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

**show ip bgp community**

The `show ip bgp community` command displays route information for the communities listed in the specified community.

**Syntax**

```
show ip bgp [vrf vrf-name] community communities [exact-match]
```

- `vrf vrf-name`—Displays the aggregate address information associated with the named VRF.

- `communities`—A string of zero or more community values, which may be in either format and may contain the community keywords `no-advertise` and `no-export`. The output displays routes that belong to every community specified in the command.

- `exact-match`—Only displays routes that are members of the communities specified in the command.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec and Global Configuration

**User Guidelines**
If the vrf argument is specified, the community information for that VRF is displayed.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
```
console#show ip bgp community
```

```
BGP table version is 0, local router ID is 65.1.1.1
Status Codes: s suppressed, * valid, > best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

Network             Next Hop         Metric     LocPref    Path          Origin
------------------ --------------- ---------- ---------- ------------- ---
```

**show ip bgp community-list**
The `show ip bgp community-list` command lists the routes that are allowed by the specified community list.

**Syntax**
```
show ip bgp [vrf vrf-name] community-list { name [exact-match]}
```
- vrf vrf-name—Displays the route information associated with the named VRF.
- name—A standard community list name.
- exact-match—(Optional) Only displays routes that are members of those and only those communities specified in the command.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec and Global Config modes

**User Guidelines**
If the vrf argument is specified, the community list information pertaining to that VRF is displayed.

**Command History**
Introduced in version 6.2.0.1 firmware. Updated in the version 6.3.0.1 firmware.

**Example**
```console
console(config)#show ip bgp community-list test
```

```
BGP table version is 0, local router ID is 65.1.1.1
Status Codes: s suppressed, * valid, > best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete
```

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------</td>
<td>----------</td>
<td>--------</td>
<td>---------</td>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>

**show ip bgp extcommunity-list**
Use the `show ip bgp extcommunity-list` command to display all the permit and deny attributes of the given extended community list. If the list-number is specified, the output is displayed that matches the given list-number; else all the lists are displayed.

**Syntax**
```
show ip bgp extcommunity-list list-number
```
- `list-number` — A standard extended community list number (0 to 99).

**Default Configuration**
No extended community lists are configured by default.
Command Mode
Privileged Exec and Global Config modes

User Guidelines
The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard extended</td>
<td>The standard named extended community list.</td>
</tr>
<tr>
<td>community-list</td>
<td></td>
</tr>
<tr>
<td>permit</td>
<td>Permits access for a matching condition. Once a permit value has been</td>
</tr>
<tr>
<td></td>
<td>configured to match a given set of extended communities the extended</td>
</tr>
<tr>
<td></td>
<td>community list defaults to an implicit deny for all other values.</td>
</tr>
<tr>
<td>RT</td>
<td>The route target extended community attribute.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access for a matching condition.</td>
</tr>
</tbody>
</table>

Command History
Introduced in version 6.3.0.1 firmware.

Example

```console
console#show ip bgp extcommunity-list 1

Standard extended community-list list1
permit RT:1:100 RT:2:100
deny RT:6:600
permit RT:5:200
permit S00:9:900
```

show ip bgp listen range
Use the `show ip bgp listen range` command to display information about IPv4 BGP listen ranges.

Syntax

`show ip bgp [vrf vrf-name] listen range [ network/length ]`

- `network/length` — Displays information about the specified listen range.
- `vrf-name` — The name of a previously configured VRF.
Default Configuration
By default, all listen ranges are shown.

Command Mode
Privileged Exec and global configuration mode

User Guidelines
There are no user guidelines.

Command History
Introduced in version 6.3.0.1 firmware.

Example
```console
console(config-router)#show ip bgp listen range

Listen Range .................................. 10.27.0.0/16
Inherited Template ............................ template_10_27

<table>
<thead>
<tr>
<th>Member</th>
<th>ASN</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.27.8.189</td>
<td>65001</td>
<td>OPENCONFIRM</td>
</tr>
<tr>
<td>10.27.128.235</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Listen Range .................................. 15.15.0.0/24
Inherited Template ............................ template_15_15

<table>
<thead>
<tr>
<th>Member</th>
<th>ASN</th>
<th>State</th>
</tr>
</thead>
</table>

show ip bgp neighbors
The show ip bgp neighbors command shows details about BGP neighbor configuration and status.

Syntax
show ip bgp [vrf vrf-name] neighbors [neighbor-address]
- neighbor-address—(Optional) The IPv4 address of a neighbor. Used to limit the output to a single neighbor.
• `vrf vrf-name` — Displays the aggregate address information associated with the named VRF.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**

Since IPv4 prefixes can only be exchanged over IPv4 peering, the neighbor-address parameter must be an IPv4 peer address. This option limits the output to show a single neighbor. If no neighbor address is specified, the command shows all neighbors enabled for IPv4 prefix exchange.

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>The neighbor’s IP address</td>
</tr>
<tr>
<td>Remote AS</td>
<td>The neighbor’s autonomous system number</td>
</tr>
<tr>
<td>Peer ID</td>
<td>The neighbor’s BGP router ID</td>
</tr>
<tr>
<td>Peer Admin Status</td>
<td>START or STOP</td>
</tr>
<tr>
<td>Peer State</td>
<td>The adjacency state of this neighbor</td>
</tr>
<tr>
<td>Local Port</td>
<td>TCP port number on the local end of the connection</td>
</tr>
<tr>
<td>Remote Port</td>
<td>TCP port number on the remote end of the connection</td>
</tr>
<tr>
<td>Connection Retry Interval</td>
<td>How long BGP waits between connection retries</td>
</tr>
</tbody>
</table>
**Neighbor Capabilities**
Optional capabilities reported by the neighbor, recognized and accepted by this router. Codes listed in the show output are as follows:

- **MP**: Multiprotocol
- **RF**: Route Refresh

This version of Dell EMC Networking does not support any multiprotocol AFI/SAFI pairs other than IPv4 unicast. The presence of this capability does not imply otherwise.

**Next Hop Self**
If the local router is configured to advertise one of its own IP addresses as the BGP Next Hop when advertising a path learned from an external peer.

**Update Source**
The configured value for the source IP address of packets sent to this peer. This field is only included in the output if the update source is configured.

**Local Interface Address**
The IPv4 address used as the source IP address in packets sent to this neighbor.

**Configured Hold Time**
The time, in seconds, that this router proposes to this neighbor as the hold time.

**Configured Keep Alive Time**
The configured KEEPALIVE interval for this neighbor.

**Negotiated Hold Time**
The minimum configured hold time and the hold time in the OPEN message received from this neighbor. If the local router does not receive a KEEPALIVE or UPDATE message from this neighbor within this interval of time, the local router drops the adjacency. This field is only shown if the adjacency state is OPEN CONFIRM or greater.

**Keep Alive Time**
The number of seconds between KEEPALIVE messages sent to this neighbor. This field is only shown if the adjacency state is OPEN CONFIRM or greater.

**Prefix Limit**
The maximum number of prefixes this router is willing to accept from this neighbor.

**Prefix Warning Threshold**
Percentage of the prefix limit that causes a warning message to be logged.
If the router receives an UPDATE message with an invalid path attribute, the router will in most cases send a NOTIFICATION message and reset the adjacency. BGP maintains a per-neighbor counter for each type of path attribute error. This show command lists each non-zero counter, just after the LastSubError. The counters that may be listed are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning Only on Prefix Limit</td>
<td>Whether to shutdown a neighbor that exceeds the prefix limit. TRUE if the event is logged without shutting down the neighbor.</td>
</tr>
<tr>
<td>Minimum Advertisement Interval</td>
<td>The minimum time between UPDATE messages sent to this neighbor.</td>
</tr>
<tr>
<td>MD5 Password</td>
<td>The TCP MD5 password, if one is configured, in plain text.</td>
</tr>
<tr>
<td>Last Error</td>
<td>The last error that occurred on the connection to this neighbor.</td>
</tr>
<tr>
<td>Last SubError</td>
<td>The suberror reported with the last error.</td>
</tr>
<tr>
<td>Established Transitions</td>
<td>The number of times the adjacency has transitioned into the Established state.</td>
</tr>
<tr>
<td>Established Time</td>
<td>How long since the connection last transitioned to or from the Established state.</td>
</tr>
<tr>
<td>Time Elapsed Since Last Update</td>
<td>How long since an UPDATE message has been received from this neighbor.</td>
</tr>
<tr>
<td>Message Table</td>
<td>The number of BGP messages sent to and received from this neighbor.</td>
</tr>
<tr>
<td>Prefixes Advertised</td>
<td>A running count of the number of prefixes advertised to or received from this neighbor.</td>
</tr>
<tr>
<td>Prefixes Withdrawn</td>
<td>A running count of the number of prefixes included in the Withdrawn Routes portion of UPDATE messages, to and from this neighbor.</td>
</tr>
<tr>
<td>Prefixes Current</td>
<td>The number of prefixes currently advertised to or received from this neighbor.</td>
</tr>
<tr>
<td>Max NLRI per Update</td>
<td>The maximum number of prefixes included in a single UPDATE message, to and from this neighbor.</td>
</tr>
<tr>
<td>Min NLRI per Update</td>
<td>The minimum number of prefixes included in a single UPDATE message, to and from this neighbor.</td>
</tr>
<tr>
<td>Counters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Path with duplicate attribute</td>
<td>The peer sent an UPDATE message containing the same path attribute more than once.</td>
</tr>
<tr>
<td>Path with well-known optional conflict</td>
<td>A received path attribute was flagged as both well-known and optional or neither well-known nor optional.</td>
</tr>
<tr>
<td>Transitive flag not set on transitive attr</td>
<td>A received path attribute is known to be transitive, but the transitive flag is not set.</td>
</tr>
<tr>
<td>Mandatory attribute non-transitive or partial</td>
<td>A mandatory path attribute was received with either the transitive or partial flag set.</td>
</tr>
<tr>
<td>Optional attribute non-transitive and partial</td>
<td>An optional path attribute has the transitive flag clear and the partial flag set.</td>
</tr>
<tr>
<td>Path attribute too long</td>
<td>A received path attribute was longer than the expected length.</td>
</tr>
<tr>
<td>Path attribute length error</td>
<td>A received path attribute has a length value that exceeds the remaining length of the path attributes field.</td>
</tr>
<tr>
<td>Invalid ORIGIN code</td>
<td>A received UPDATE message included an invalid ORIGIN code.</td>
</tr>
<tr>
<td>Unexpected first ASN in AS path</td>
<td>The AS Path attribute from an external peer did not include the peer’s AS number as the first AS.</td>
</tr>
<tr>
<td>Invalid AS path segment type</td>
<td>The AS Path includes a segment with an invalid segment type.</td>
</tr>
<tr>
<td>Invalid BGP NEXT HOP</td>
<td>The BGP NEXT HOP is not a valid unicast address.</td>
</tr>
<tr>
<td>Bad BGP NEXT HOP</td>
<td>The BGP NEXT HOP was either the receiver’s IP address or an IP address outside the subnet to the peer.</td>
</tr>
<tr>
<td>Invalid AGGREGATOR attribute</td>
<td>The AGGREGATOR attribute was invalid.</td>
</tr>
<tr>
<td>Unrecognized well-known path attribute</td>
<td>An UPDATE message contained a path attribute with the Optional flag clear, but this router does not recognize the attribute.</td>
</tr>
<tr>
<td>Missing mandatory path attribute</td>
<td>An UPDATE message was received without a mandatory path attribute.</td>
</tr>
<tr>
<td>Missing LOCAL PREF attribute</td>
<td>An UPDATE message was received from an internal peer without the LOCAL PREF attribute.</td>
</tr>
</tbody>
</table>
Invalid prefix in UPDATE NLRI

An UPDATE message received from this peer contained a syntactically incorrect prefix.

**Command History**

Introduced in version 6.2.0.1 firmware.

Updated in version 6.3.0.1 firmware.

**Example**

```console
console#show ip bgp neighbors

Remote Address ................................ 10.10.10.10
Remote AS .................................. 65000
Peer ID .................................... 0.0.0.0
Peer Admin Status .......................... START
Peer State .................................. IDLE
Local Interface Address ..................... 10.10.10.3
Local Port .................................. 179
Remote Port .................................. 54474
Connection Retry Interval ................... 2 sec
Neighbor Capabilities ....................... None
Next Hop Self ............................... Disable
IPv4 Unicast Support ........................ Sent
IPv6 Unicast Support ........................ None
Template Name ............................... None
Update Source ............................... None
Configured Hold Time ....................... None
Configured Keep Alive Time ................. None
Prefix Limit ............................... 8160
Prefix Warning Threshold ................... 75
Warning Only On Prefix Limit .............. False
MD5 Password ............................... None
Originate Default ........................... False

Last Error (Sent) ............................. OPEN Message Error
Last SubError ............................... Bad Peer AS
Time Since Last Error ....................... 0 days 00 hrs 00 mins 02 secs
Established Transitions .................... 0
Established Time ............................ 0 days 01 hrs 45 mins 20 secs
Time Since Last Update ..................... No UPDATE received
IPv4 Outbound Update Group ............... None

<table>
<thead>
<tr>
<th>Open</th>
<th>Update</th>
<th>Keepalive</th>
<th>Notification</th>
<th>Refresh</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msgs Sent</td>
<td>2287</td>
<td>0</td>
<td>0</td>
<td>2122</td>
<td>0</td>
</tr>
<tr>
<td>Msgs Rcvd</td>
<td>2122</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Received UPDATE Queue Size: 0 bytes. High: 0 Limit: 392192 Drops: 0
IPv4 Prefix Statistics:

<table>
<thead>
<tr>
<th></th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes Advertised</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Withdrawn</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Current</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Accepted</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Prefixes Rejected</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Max NLRI per Update</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Min NLRI per Update</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

console # show ip bgp neighbors 172.20.1.100

Remote Address ........................................ 172.20.1.100
Remote AS .................................................. 100
Peer ID ...................................................... 14.3.0.1
Peer Admin Status ........................................ START
Peer State .................................................... ESTABLISHED
Local Port ................................................... 179
Remote Port .................................................. 58265
Connection Retry Interval ............................... 120 sec
Neighbor Capabilities ...................................... None
Next Hop Self ............................................... Disable
Update Source................................................
Local Interface Address ................................... 172.20.1.2
Configured Hold Time ....................................... 90 sec
Configured Keep Alive Time ............................... 30 sec
Negotiated Hold Time ....................................... 30 sec
Keep Alive Time ............................................. 10 sec
Prefix Limit ............................................... None
Prefix Warning Threshold ................................. 75%
Warning Only On Prefix Limit ............................. TRUE
Minimum Advertisement Interval .......................... 30 sec
MD5 Password ................................................. password
Originate Default .......................................... TRUE

Last Error (Sent)............................................. Hold Timer Expired
Last SubError................................................ None
Time Since Last Error ...................................... 0 day 0 hr 4 min 27 sec
Established Transitions .................................... 1
Established Time ............................................ 0 day 0 hr 4 min 25 sec
Time Since Last Update .................................... 0 day 0 hr 4 min 25 sec
Outbound Update Group .................................... 3

<table>
<thead>
<tr>
<th></th>
<th>Open</th>
<th>Update</th>
<th>Keepalive</th>
<th>Notification</th>
<th>Refresh</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msgs Sent</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>Msgs Rcvd</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes Advertised</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
In this example, BGP has received an UPDATE message from an external peer 172.20.101.100 with something other than the peer’s ASN as the first ASN in the AS Path. The additional counter shows that this occurred one time.

```console
console #show ip bgp neighbors 172.20.101.100

Remote Address ................................ 172.20.101.100
Remote AS ..................................... 101

Last Error .................................... UPDATE Message Error
Last SubError ................................. Malformed AS_PATH
Unexpected first ASN in AS path ............... 1

Established Transitions ....................... 1
Established Time .............................. 0 days 00 hrs 00 mins 10 secs
```

**show ip bgp neighbors advertised-routes**

The `show ip bgp neighbors advertised-routes` command displays the list of routes advertised to a specific neighbor. These are the routes in the adjacent RIB out for the neighbor’s outbound update group

**Syntax**

```
show ip bgp [vrf vrf-name] neighbors ip-address advertised-routes
```

- **ip-address**—The IPv4 address of a neighbor.
- **vrf vrf-name** — Displays the aggregate address information associated with the named VRF.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

Privileged Exec mode, Global Configuration mode, and all sub-modes
User Guidelines

Note that this output differs slightly from the output in `show ip bgp`. Suppressed routes and non-best routes are not advertised; so these status codes are not relevant here. Advertised routes always have a single next hop, the BGP NEXT HOP advertised to the peer. Local preference is never sent to external peers.

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The output indicates whether BGP is configured to originate a default route to this peer (`neighbor default-originate`).

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.</td>
</tr>
<tr>
<td>Status codes</td>
<td>p—The route has been updated in Adj-RIB-Out since the last UPDATE message was sent. Transmission of an UPDATE message is pending.</td>
</tr>
<tr>
<td>Network</td>
<td>Destination prefix</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The BGP NEXT HOP as advertised to the peer.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The local preference. Local preference is never advertised to external peers.</td>
</tr>
<tr>
<td>Metric</td>
<td>The value of the Multi Exit Discriminator, if the MED is advertised to the peer.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path. The AS path does not include the local AS number, which is added to the beginning of the AS path when a route is advertised to an external peer.</td>
</tr>
<tr>
<td>Origin</td>
<td>The value of the Origin attribute.</td>
</tr>
</tbody>
</table>

Command History

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

Example

```console
console#show ip bgp neighbors 10.10.10.10 advertised-routes
```
BGP table version is 5, local router ID is 0.0.0.100
Status codes: p - advertisement pending
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.1.0/24</td>
<td>172.20.101.1</td>
<td>10</td>
<td>100</td>
<td>20 10</td>
<td>i</td>
</tr>
<tr>
<td>p 20.1.1.0/24</td>
<td>172.20.101.1</td>
<td>100</td>
<td>20</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors received-routes**

This command displays the list of routes received from a specific neighbor. The list includes both the accepted and rejected routes.

**Syntax**

show ip bgp [vrf vrf-name]neighbors ip-address {received-routes | routes | rejected-routes}

- vrf vrf-name — Displays the aggregate address information associated with the named VRF.
- ip-address—The IPv4 address of a BGP neighbor.
- Received-routes—Display the routes received by a particular neighbor prior to filtering.
- Routes—Display both the received and advertised routes.
- Rejected-routes—Display the routes rejected from the specified neighbor.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes

**User Guidelines**

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following fields are displayed.
### Layer 3 Routing Commands

#### Command History

Introduced in version 6.2.0.1 firmware.

Updated in version 6.3.0.1 firmware.

#### Example

```console
console #show ip bgp neighbors 172.20.101.100 received-routes

local router ID is 20.1.1.1
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>Local Pref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.1.0/24</td>
<td>172.20.101.1</td>
<td>10</td>
<td>100</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>172.20.101.1</td>
<td></td>
<td></td>
<td>100</td>
<td>20</td>
</tr>
</tbody>
</table>
```

```console
console #show ip bgp neighbors 10.10.10.3 routes

Local router ID is 0.0.0.101
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPref</th>
<th>Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>10.10.10.3</td>
<td>1</td>
<td></td>
<td>65001</td>
<td>i</td>
</tr>
<tr>
<td>1.2.0.0/16</td>
<td>10.10.10.3</td>
<td>0</td>
<td></td>
<td>65001</td>
<td>i</td>
</tr>
<tr>
<td>1.2.3.0/24</td>
<td>10.10.10.3</td>
<td>0</td>
<td></td>
<td>65001</td>
<td>i</td>
</tr>
</tbody>
</table>
```

#### Fields and Description

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Destination prefix</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The BGP NEXT HOP as advertised by the peer.</td>
</tr>
<tr>
<td>Metric</td>
<td>The value of the Multi Exit Discriminator, if a MED is received from the peer.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The local preference received from the peer.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path as received from the peer</td>
</tr>
<tr>
<td>Origin</td>
<td>The value of the Origin attribute as received from the peer follows immediately after the AS PATH.</td>
</tr>
</tbody>
</table>
**show ip bgp neighbors policy**

This command displays the inbound and outbound IPv4 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

**Syntax**

`show ip bgp [vrf vrf-name] neighbors ip-address policy`

- **vrf vrf-name** — Displays the aggregate address information associated with the named VRF.
- **ip-address**—The IPv4 address of a neighbor can optionally be specified to limit the output to a single neighbor.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes

**User Guidelines**

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following fields are displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>The peer address of a neighbor.</td>
</tr>
<tr>
<td>Policy</td>
<td>A neighbor-specific BGP policy.</td>
</tr>
<tr>
<td>Template</td>
<td>If the policy is inherited from a peer template, this field lists the template name.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

Updated in version 6.3.0.1 firmware.
Example

console #show ip bgp neighbors 172.20.101.100 policy

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Policy</th>
<th>Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.101.100</td>
<td>advertisement-interval 600</td>
<td></td>
</tr>
<tr>
<td></td>
<td>default-originate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter-list 500 in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter-list 500 out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-list barney in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-list wilma out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>maximum-prefix unlimited 100 warning-only</td>
<td>torPeers</td>
</tr>
<tr>
<td></td>
<td>route-map fred in</td>
<td>torPeers</td>
</tr>
<tr>
<td></td>
<td>route-map dino out</td>
<td>torPeers</td>
</tr>
<tr>
<td></td>
<td>send-community</td>
<td>torPeers</td>
</tr>
<tr>
<td></td>
<td>advertisement-interval 600</td>
<td>torPeers</td>
</tr>
<tr>
<td></td>
<td>default-originate</td>
<td>torPeers</td>
</tr>
</tbody>
</table>

**show ip bgp route-reflection**

This command displays all global configuration related to IPv4 route reflection, including the cluster ID and whether client-to-client route reflection is enabled, and lists all the neighbors that are configured as route reflector clients.

**Syntax**

show ip bgp [vrf vrf-name] route-reflection

- vrf vrf-name — Displays the aggregate address information associated with the named VRF.

**Default Configuration**

By default, information about the global VRF is shown.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes

**User Guidelines**

If a route reflector client is configured with an outbound route map, the output warns that set statements in the route map are ignored when reflecting routes to this client.
If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following information is displayed:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>The cluster ID used by this router. The value is tagged as configured when the value is configured with the <code>bgp cluster-id</code> command. When no cluster ID is configured, the local router ID is shown and tagged as default.</td>
</tr>
<tr>
<td>Client-to-client reflection</td>
<td>Displayed as Enabled when this router reflects routes received from its clients to its other clients. Otherwise, disabled.</td>
</tr>
<tr>
<td>Clients</td>
<td>A list of this router’s internal peers which have been configured as route reflector clients.</td>
</tr>
<tr>
<td>Non-client Internal Peers</td>
<td>A list of this router’s internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

Updated in version 6.3.0.1 firmware.

**Example**

```
console # show ip bgp route-reflection

Cluster ID......................... 1.1.1.1 (configured)
Client-to-client Reflection....... Enabled
Clients:  172.20.1.2, 172.20.3.2, 172.20.5.2
Non-client Internal Peers:  192.168.1.2, 192.168.2.2

Skipping set statements in outbound route map gandolf when reflecting to internal peer 172.20.1.2.
```

**show ip bgp statistics**

This command displays recent decision process history. Phase 1 of the decision process reacts to UPDATE messages received from peers, determining what new routes are accepted and deleting withdrawn routes from the Adj-RIB-In. Phase 2 determines the best path for each destination,
updates the BGP route table, and updates the common RIB. Phase 3 is run independently for each outbound update group and determines which routes should be advertised to neighbors in each group. Each entry in the table shows statistics for one phase of the decision process. The table shows the 20 most recent decision process runs, with the most recent information at the end of the table.

Syntax

```
show ip bgp [vrf vrf-name] statistics
```

- `vrf vrf-name` — Displays the aggregate address information associated with the named VRF.

Default Configuration

By default, information about the global VRF is shown.

Command Mode

User Exec mode, Privileged Exec mode, Global Config mode and all sub-modes.

User Guidelines

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>How long since the decision process was run. hours:minutes:seconds if the elapsed time is less than 24 hours. Otherwise, days:hours.</td>
</tr>
<tr>
<td>Phase</td>
<td>The phase of the decision process that was run.</td>
</tr>
<tr>
<td>Upd Grp</td>
<td>Outbound update group ID. Only applies when phase 3 is run.</td>
</tr>
<tr>
<td>GenId</td>
<td>Generation ID of BGP routing table when decision process was run. The generation ID is incremented each time phase 2 of the decision process is run and when there is a change to the status of aggregate addresses.</td>
</tr>
</tbody>
</table>
show ip bgp summary

This command displays a summary of BGP configuration and status.

Syntax

show ip bgp [vrf vrf-name] summary
• **vrf vrf-name** — Displays the aggregate address information associated with the named VRF.

### Default Configuration

By default, information about the global VRF is shown.

### Command Mode

User Exec mode, Privileged Exec mode, Global Config mode and all sub-modes.

### User Guidelines

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>Whether BGP is globally enabled.</td>
</tr>
<tr>
<td>BGP Router ID</td>
<td>The configured router ID</td>
</tr>
<tr>
<td>Local AS Number</td>
<td>The router’s AS number</td>
</tr>
<tr>
<td>Traps</td>
<td>Whether BGP traps are enabled.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an external BGP route.</td>
</tr>
<tr>
<td>Maximum Paths iBGP</td>
<td>The maximum number of next hops in an internal BGP route.</td>
</tr>
<tr>
<td>Default Keep Alive Time</td>
<td>The configured keepalive time used by all peers that have not been configured with a peer-specific keepalive time.</td>
</tr>
<tr>
<td>Default Hold Time</td>
<td>The configured hold time used by all peers that have not been configured with a peer-specific hold time.</td>
</tr>
<tr>
<td>Number of Network Entries</td>
<td>The number of distinct prefixes in the local RIB.</td>
</tr>
<tr>
<td>Number of AS Paths</td>
<td>The number of AS paths in the local RIB.</td>
</tr>
<tr>
<td>Dynamic Neighbors</td>
<td>The number of dynamically discovered neighbors (current number, maximum number discovered, upper limit allowed).</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Metric</td>
<td>The default value for the MED for redistributed routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether BGP is configured to advertise a default route. Corresponds to default-information originate.</td>
</tr>
</tbody>
</table>

**Redistributing**

<table>
<thead>
<tr>
<th>Source</th>
<th>A source of routes that BGP is configured to redistribute.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>The metric configured with the redistribute command.</td>
</tr>
<tr>
<td>Match Value</td>
<td>For routes redistributed from OSPF, the types of OSPF routes being redistributed.</td>
</tr>
<tr>
<td>Distribute List</td>
<td>The name of the prefix list used to filter redistributed routes, if one is configured with the distribute-list out command.</td>
</tr>
<tr>
<td>Route Map</td>
<td>The name of the route map used to filter redistributed routes.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The IP address of a neighbor.</td>
</tr>
<tr>
<td>ASN</td>
<td>The neighbor's ASN.</td>
</tr>
<tr>
<td>MsgRecvd</td>
<td>The number of BGP messages received from this neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>The number of BGP messages sent to this neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>The adjacency state. One of IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST.</td>
</tr>
<tr>
<td>Up/Down Time</td>
<td>How long the adjacency has been in the ESTABLISHED state, or, if the adjacency is down, how long it has been down. In days:hours:minutes:seconds.</td>
</tr>
<tr>
<td>Pfx Recvd</td>
<td>The number of prefixes received from the neighbor.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

Updated in version 6.3.0.1 firmware.
Example

console#show ip bgp summary

IPv4 Routing .................................. Enable
BGP Admin Mode ................................ Enable
BGP Router ID .................................. 0.0.0.100
Local AS Number ............................... 65001
Traps ......................................... Disable
Maximum Paths ................................. 1
Maximum Paths iBGP ............................ 1
Default Keep Alive Time ....................... 30
Default Hold Time .............................. 90
Number of Network Entries ..................... 3
Number of AS Paths ............................. 0
Dynamic Neighbors Current/High/Limit ........ 1/1/20
Default Metric ................................. Not Configured
Default Route Advertise ....................... No

Redistributing:
Source    Metric     Dist List                        Route Map
--------- ---------- -------------------------------- ----------------------
static
ospf     300
        ospf match: int

Neighbor         ASN  MsgRcvd  MsgSent  State         Up/Down Time    Pfx Rcvd
---------------- ----- -------- -------- ------------- -------------- ------
10.10.10.10      65000 2269    4666     ESTABLISHED   0:00:17:15     0

show ip bgp template

The show ip bgp template command lists the routes that are allowed by the specified community list.

Syntax

show ip bgp template [ template-name ]

- template-name—(Optional) Limits the output to a single template

Default Configuration

There is no default configuration for this command.
**Command Mode**
Privileged Exec mode

**User Guidelines**
The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>The name of a BGP peer template.</td>
</tr>
<tr>
<td>AF</td>
<td>The address family to which the configuration command applies. This field is blank for session parameters, which apply to all address families.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configuration commands that are included in the template.</td>
</tr>
</tbody>
</table>

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console#show ip bgp template

Template Name   AF                     Configuration
--------------- -----------------------------------------------------------
peer-grp1        timers 5 15           password rivendell
                 IPv4                    advertisement-interval 15

peer-grp2        IPv4                   prefix-list strider in
                 IPv4                    maximum-prefix 100
                 IPv6                    prefix-list gandolf in
                 IPv6                    maximum-prefix 200

peer-grp3        IPv6                   send-community

peer-grp4        IPv4                    update-source loopback 0
                 IPv4                    next-hop-self
```

**show ip bgp traffic**
The `show ip bgp traffic` command list the routes that are allowed by the specified community list.
Syntax
show ip bgp [vrf vrf-name] traffic

- vrf vrf-name — Displays the aggregate address information associated with the named VRF.

Default Configuration
By default, information about the global VRF is shown.

Command Mode
User Exec mode, Privileged Exec mode, Global Configuration mode and all sub-modes.

User Guidelines
If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The output shows when BGP counters were last cleared (using clear ip bgp counters). Clearing counters resets all values in this output to 0 except for the high water mark for the work queues.

The first table lists the number of BGP messages of each type that this router has sent and received. Following the table is a maximum send and receive UPDATE message rate. These rates report the busiest one-second interval.

The queue statistics table reports information for BGP work queues. Items placed on each of these work queues are as follows:

- The Events queue includes most timer events and configuration changes.
- The Keepalive Tx queue includes timer events to send a KEEPALIVE message to a peer. The Dec Proc queue includes events that cause the decision process to be run.
- The Rx Data queue holds incoming BGP messages.
- The RTO Notifications queue includes best route change and next hop resolution change notifications from the routing table.
- The MIB Queries queue includes pending SNMP queries for BGP status.

Command History
Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

**Example**

```
console#show ip bgp traffic
```

Time Since Counters Cleared: 55223 Seconds
BGP Message Statistics

<table>
<thead>
<tr>
<th></th>
<th>Recd:</th>
<th>Update</th>
<th>Notification</th>
<th>Keepalive</th>
<th>Refresh</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recd:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7905</td>
</tr>
<tr>
<td>Sent:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8532</td>
</tr>
</tbody>
</table>

Max Received UPDATE rate: 1 pps
Max Send UPDATE rate: 5 pps

BGP Queue Statistics

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Max</th>
<th>Drops</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>800</td>
</tr>
<tr>
<td>Keepalive Tx</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>128</td>
</tr>
<tr>
<td>Dec Proc</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>133</td>
</tr>
<tr>
<td>Rx Data</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>RTO Notifications</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>1222</td>
</tr>
<tr>
<td>MIB Queries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>

**show ip bgp update-group**

This command reports the status of IPv4 outbound update groups and their members.

**Syntax**

```
show ip bgp [vrf vrf-name] update-group [group-index | peer-address]
```

- **vrf vrf-name** — Displays the aggregate address information associated with the named VRF.
- **group-index**—(Optional) If specified, this option restricts the output to a single update group.
- **peer-address**—(Optional) If specified, this option restricts the output to the update group containing the peer with the given IPv4 address.

**Default Configuration**

By default, information about the global VRF is shown.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes

**User Guidelines**

If the vrf-name argument is specified, information pertaining to that VRF is displayed.

The update send history table show statistics on as many as the fifteen most recent executions of the update send process for the update group. Items in the history table are as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The update version.</td>
</tr>
<tr>
<td>Delta T</td>
<td>The amount of time elapsed since the update send process executed. hours::minutes::seconds.</td>
</tr>
<tr>
<td>Duration</td>
<td>How long the update send process took, in milliseconds</td>
</tr>
<tr>
<td>UPD Built</td>
<td>The number of UPDATE messages built.</td>
</tr>
<tr>
<td>UPD Sent</td>
<td>The number of UPDATE messages successfully transmitted to group members. Normally a copy of each UPDATE message built is sent to each group member.</td>
</tr>
<tr>
<td>Paths Sent</td>
<td>The number of paths advertised.</td>
</tr>
<tr>
<td>Pfxs Adv</td>
<td>The number of prefixes advertised.</td>
</tr>
<tr>
<td>Pfxs Wd</td>
<td>The number of prefixes withdrawn.</td>
</tr>
</tbody>
</table>

The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Group ID</td>
<td>Unique identifier for outbound update group.</td>
</tr>
<tr>
<td>Peer Type</td>
<td>Whether peers in this update group are internal or external.</td>
</tr>
<tr>
<td>Minimum Advertisement Interval</td>
<td>The minimum time, in seconds, between sets of UPDATE messages sent to the group.</td>
</tr>
<tr>
<td>Send Community</td>
<td>Whether BGP communities are included in route advertisements to members of the group. Yes or No.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Neighbor AS Path Access List Out</td>
<td>The AS path access list used to filter UPDATE messages sent to peers in the update group.</td>
</tr>
<tr>
<td>Neighbor Prefix List Out</td>
<td>Name of the prefix list used to filter prefixes advertised to the peers in the update group.</td>
</tr>
<tr>
<td>Neighbor Route Map Out</td>
<td>Name of the route map used to filter and modify routes advertised to the peers in the update group.</td>
</tr>
<tr>
<td>Members Added</td>
<td>The number of peers added to the group since the group was formed.</td>
</tr>
<tr>
<td>Members Removed</td>
<td>The number of peers removed from the group.</td>
</tr>
<tr>
<td>Update Version</td>
<td>The number of times phase 3 of the BGP decision process has run for this group to determine which routes should be advertised to the group.</td>
</tr>
<tr>
<td>Number of UPDATEs Sent</td>
<td>The number of UPDATE messages that have been sent to this group. Incremented once for each UPDATE regardless of the number of group members.</td>
</tr>
<tr>
<td>Time Since Last UPDATE</td>
<td>Time since an UPDATE message was last sent to the group. If no UPDATE has been sent to the group, the status is “Never.”</td>
</tr>
<tr>
<td>Current Prefixes</td>
<td>The number of prefixes currently advertised to the group.</td>
</tr>
<tr>
<td>Current Paths</td>
<td>The number of paths currently advertised to the group.</td>
</tr>
<tr>
<td>Prefixes Advertised</td>
<td>The total number of prefixes advertised to the group since the group was formed.</td>
</tr>
<tr>
<td>Prefixes Withdrawn</td>
<td>The total number of prefixes included in the Withdrawn Routes field of UPDATE messages sent to the group since the group was formed.</td>
</tr>
<tr>
<td>UPDATE Send Failures</td>
<td>The number of UPDATE messages that failed to be delivered to all members of the group.</td>
</tr>
<tr>
<td>Current Members</td>
<td>The IPv4 address of all current members of the group.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.
Example

console# show ip bgp update-group

Update Group ID........................................... 0
Peer Type.................................................. External
Minimum Advertisement Interval.................. 30 seconds
Send Community.......................................... Yes
Neighbor AS Path Access List Out................. 1
Neighbor Prefix List Out.............................. prefixList1
Neighbor Route Map Out............................... None
Members Added............................................. 48
Members Removed......................................... 0
Update Version........................................... 19
Number of UPDATEs Sent.............................. 512
Time Since Last Update............................... 5 hrs 3 min 2 sec
Current Prefixes........................................ 5500
Current Paths............................................. 22
Prefixes Advertised.................................... 191250
Prefixes Withdrawn..................................... 186000
UPDATE Send Failures................................. 0

Current Members: 172.20.1.100, 172.20.2.100

<table>
<thead>
<tr>
<th>Version</th>
<th>Delta T</th>
<th>Duration</th>
<th>UPD Built</th>
<th>UPD Sent</th>
<th>Paths Sent</th>
<th>Pfxs Adv</th>
<th>Pfxs Wd</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>00:33:49</td>
<td>100</td>
<td>6</td>
<td>288</td>
<td>5</td>
<td>1250</td>
<td>750</td>
</tr>
<tr>
<td>11</td>
<td>00:33:49</td>
<td>0</td>
<td>4</td>
<td>192</td>
<td>3</td>
<td>750</td>
<td>250</td>
</tr>
<tr>
<td>12</td>
<td>00:33:49</td>
<td>0</td>
<td>2</td>
<td>96</td>
<td>1</td>
<td>250</td>
<td>1000</td>
</tr>
<tr>
<td>13</td>
<td>00:33:49</td>
<td>0</td>
<td>2</td>
<td>96</td>
<td>1</td>
<td>250</td>
<td>1018</td>
</tr>
<tr>
<td>14</td>
<td>00:33:49</td>
<td>0</td>
<td>1</td>
<td>48</td>
<td>0</td>
<td>0</td>
<td>482</td>
</tr>
<tr>
<td>15</td>
<td>00:33:49</td>
<td>100</td>
<td>8</td>
<td>384</td>
<td>7</td>
<td>1750</td>
<td>750</td>
</tr>
<tr>
<td>16</td>
<td>00:33:49</td>
<td>0</td>
<td>3</td>
<td>144</td>
<td>2</td>
<td>500</td>
<td>250</td>
</tr>
<tr>
<td>17</td>
<td>00:31:49</td>
<td>0</td>
<td>4</td>
<td>192</td>
<td>3</td>
<td>750</td>
<td>750</td>
</tr>
<tr>
<td>18</td>
<td>00:23:49</td>
<td>100</td>
<td>4</td>
<td>192</td>
<td>3</td>
<td>750</td>
<td>1000</td>
</tr>
<tr>
<td>19</td>
<td>00:03:49</td>
<td>100</td>
<td>6</td>
<td>288</td>
<td>5</td>
<td>1250</td>
<td>500</td>
</tr>
</tbody>
</table>

Update Group ID........................................... 1
Peer Type.................................................. Internal
Minimum Advertisement Interval.................. 5 seconds
Send Community.......................................... Yes
Neighbor AS Path Access List Out................. none
Neighbor Prefix List Out.............................. none
Members Added............................................. 3
Members Removed......................................... 0
Update Version........................................... 4
Number of UPDATEs Sent.............................. 8
Time Since Last UPDATE............................... 3 hrs 13 min 22 sec
Current Prefixes........................................ 84
Current Paths........................................... 2
Prefixes Advertised.................................... 100
Prefixes Withdrawn.................................... 16
show ip bgp vpn4

Use the `show ip bgp vpn4` command to display the VPNv4 address information from the BGP table. If the vrf argument is specified, the address information pertaining to that VRF is displayed.

**Syntax**

```
show ip bgp vpnv4 {all | rd route-distinguisher [ipprefix/length] | vrf vrf-name [ip-prefix/length] | statistics }
```

- **all**— Displays the complete VPNv4 database.
- **rd** route-distinguisher—Displays the NLRI prefixes that match the named route distinguisher.
- **vrf** vrf-name—Displays the NLRI prefixes associated with the named VRF instance.
- **ip-prefix/length** — IP address of a network in the routing table and the length of the mask (0 to 32). The slash mark must be included.
- **statistics** — Displays BGP VPNv4 statistics

**Default Configuration**

There is no default configuration.

**Command Mode**

Privileged Exec and Global Configuration modes

**User Guidelines**

The format and field descriptions are the same as for `show ip bgp neighbors` with the following exceptions:

- If the peer address (“Remote Address”) is a link local address, the next line of output indicates the scope of the address.
- No “IPv4 Outbound Update Group” is listed.
- No IPv4 prefix statistics are shown, since this implementation does not support advertisement of IPv4 prefixes over IPv6 transport.
- “RFC 5549 Support” is displayed only if the BGP neighbor is peered over IPv6 network.
- If the peer is configured as “autodetect”, the “Remote Address” shows detected IPv6 address or “Unresolved” if the peer is not detected by the autodetect feature.
- The “Autodetect Status” field is displayed only if the peer is configured as “autodetect”. The field shows one of the following status: “Peer is detected”, “Peer is not detected” or “Multiple peers are detected”.

The command output provides the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented</td>
</tr>
<tr>
<td>Status codes</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• s: The route is aggregated into an aggregate address configured with the summary-only option.</td>
</tr>
<tr>
<td></td>
<td>• *: BGP never displays invalid routes; so this code is always displayed (to maintain consistency with the industry standard).</td>
</tr>
<tr>
<td></td>
<td>• &gt;: Indicates that BGP has selected this path as the best path to the destination.</td>
</tr>
<tr>
<td></td>
<td>• i: If the route is learned from an internal peer.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>The RD associated with the VRF.</td>
</tr>
<tr>
<td>Network</td>
<td>The destination prefix.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The route’s BGP NEXT HOP.</td>
</tr>
<tr>
<td>Metric</td>
<td>BGP metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>The local preference.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path per route.</td>
</tr>
<tr>
<td>Prefix/Prefix Length</td>
<td>The destination prefix and prefix length.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Generation ID</td>
<td>The version of the BGP routing table when this route last changed.</td>
</tr>
<tr>
<td>Forwarding</td>
<td>If this BGP route is used for forwarding.</td>
</tr>
<tr>
<td>Advertised To Update Groups</td>
<td>The outbound update groups to which this route is advertised.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>The local preference, either as received from the peer or as set according to local policy.</td>
</tr>
<tr>
<td>AS Path</td>
<td>The AS Path. This form of <code>show ip bgp</code> displays AS Paths as long as allowed by <code>bgp maxas-limit</code>.</td>
</tr>
<tr>
<td>Origin</td>
<td>Value of the ORIGIN attribute.</td>
</tr>
<tr>
<td>Metric</td>
<td>Value of the MED attribute, if included.</td>
</tr>
<tr>
<td>Type</td>
<td>Whether the path is received from an internal or external peer.</td>
</tr>
<tr>
<td>IGP Cost</td>
<td>The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP.</td>
</tr>
<tr>
<td>Peer (Peer ID)</td>
<td>The IP address of the peer that sent this route, and its router ID.</td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>The BGP NEXT HOP attribute.</td>
</tr>
<tr>
<td>Atomic Aggregate</td>
<td>If the ATOMIC AGGEGATE attribute is attached to the path.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The AS number and router ID of the speaker that aggregated the route.</td>
</tr>
<tr>
<td>Communities</td>
<td>The BGP communities attached to the path.</td>
</tr>
<tr>
<td>Originator</td>
<td>If the ORIGINATOR attribute is attached to the path, the value of this attribute.</td>
</tr>
<tr>
<td>Cluster List</td>
<td>If the CLUSTER_LIST attribute is attached to the path, the sequence of cluster IDs in the cluster list.</td>
</tr>
<tr>
<td>Extended Community</td>
<td>Route target value associated with the specified route</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.3.0.1 firmware.
Example

The following example shows all available VPNv4 information in a BGP routing table:

console#show ip bgp vpnv4 all

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 172.20.1.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
<tr>
<td>* 24.95.16.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
<tr>
<td>* 24.14.8.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
</tbody>
</table>

Route Distinguisher : 2:20 (for VRF blue)

* 173.20.1.0/24          | 120.10.1.1 | 10     | 100    | 20 10 i |
* 25.95.16.0/24          | 120.10.1.1 | 10     | 100    | 20 10 i |
* 25.14.8.0/24           | 120.10.1.1 | 10     | 100    | 20 10 i |

Route Distinguisher : 3:30 (for VRF yellow)

* 174.20.1.0/24          | 130.10.1.1 | 10     | 100    | 20 10 i |
* 26.95.16.0/24          | 130.10.1.1 | 10     | 100    | 20 10 i |
* 26.14.8.0/24           | 130.10.1.1 | 10     | 100    | 20 10 i |

The following example shows VPNv4 routing entries for VRF named red:

(R1) # show ip bgp vpnv4 vrf red

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 172.20.1.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
<tr>
<td>* 24.95.16.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
<tr>
<td>* 24.14.8.0/24</td>
<td>100.10.1.1</td>
<td>10</td>
<td>100</td>
<td>20 10 i</td>
</tr>
</tbody>
</table>

The following example shows the attributes for network 172.20.1.0 that include multi-paths and best path (Use like any of the below formats):

(R1) # show ip bgp vpnv4 vrf red 172.20.1.0/24

Prefix/Prefix Length....................... 1:100:172.20.1.0/24
Generation ID.............................. 2056
Forwarding.................................. Yes
Advertised to Update Groups................. 1, 5
Best Path:
Imported from.............................. 2:200:100.10.1.1
Local Preference........................... 100
AS Path.................................... 20 10
Origin..................................... IGP
Metric..................................... 10
Type........................................ External
IGP Cost................................... 30
Peer (Peer ID)............................. 100.10.1.1 (32.4.1.1)
BGP Next Hop............................... 100.10.1.1
Atomic Aggregate........................ Included
Aggregator (AS, Router ID)............. 300, 14.1.1.1
Communities.............................. no-export
Extended Community...................... RT:1:100
                                      RT:2:200
Originator................................ 10.1.1.1

Non-best Paths:
Local Preference........................... 200
AS Path.................................... 18 50 27
Origin..................................... Incomplete
Type........................................ External
IGP Cost................................... 10
Peer (Peer ID)............................. 200.1.1.1 (18.24.1.3)
BGP Next Hop............................... 200.1.1.1
Extended Community...................... RT:3:300

**template peer**

Use the **template peer** command in router configuration mode to create a BGP peer template and enter peer template configuration mode. To delete a peer template, use the no form of this command.

**Syntax**

```plaintext
template peer name

no template peer name
```

- name—The name of the template. The name may be no more than 32 characters.

**Default Configuration**

No peer templates are configured by default.
**Command Mode**

BGP Router Configuration mode

**User Guidelines**

A peer template can be configured with parameters that apply to many peers. Neighbors can then be configured to inherit parameters from the peer template. A peer template can include both session parameters and peer policies. Peer policies are configured within an address family configuration mode and apply only to that address family. You can configure up to 32 peer templates. When changing a template, the change is immediately applied to all neighbors that inherit from the template (though policy changes are subject to a three-minute delay.)

The following commands can be issued in peer template configuration mode and thus added to a peer template:

- address-family
- allowas-in
- connect-retry-interval
- description
- ebgp-multihop
- fall-over
- local-as
- password
- remote-as
- rfc5549-support
- shutdown
- timers
- update-source

See the associated `neighbor` commands for a description of parameters and keywords. Note that Dell EMC Networking does not support a `remote-as` as-number command in this mode. The neighbor’s AS number must be specified when the neighbor is created.
Command History
Introduced in version 6.2.0.1 firmware. Additional command options added in 6.3.0.1 firmware.

Example
console(config)# router bgp 65000
console(config-router)# neighbor 172.20.1.2 remote-as 65001
console(config-router)# neighbor 172.20.2.2 remote-as 65001
console(config-router)# template peer AGGR
console(config-rtr-tmplt)# timers 3 9
console(config-rtr-tmplt)# address-family ipv4
console(config-rtr-tmplt-af)# send-community
console(config-rtr-tmplt-af)# route-map RM4-IN in
console(config-rtr-tmplt-af)# route-map RM4-OUT out
console(config-rtr-tmplt-af)# exit
console(config-rtr-tmplt)# address-family ipv6
console(config-rtr-tmplt-af)# send-community
console(config-rtr-tmplt-af)# route-map RM6-IN in
console(config-rtr-tmplt-af)# route-map RM6-OUT out
console(config-rtr-tmplt-af)# exit
console(config-rtr-tmplt)# exit
console(config-router)# neighbor 172.20.1.2 inherit peer AGGR
console(config-router)# neighbor 172.20.2.2 inherit peer AGGR
console(config-router)# address-family ipv6
console(config-router)# neighbor 172.20.1.2 activate
console(config-router)# neighbor 172.20.2.2 activate

timers bgp
The timers bgp command configures the default keepalive and hold timers that BGP uses for all neighbors unless specifically overridden by the neighbor timers command.

Syntax
timers bgp keepalive holdtime
no timers bgp

- keepalive—The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. An small internal jitter is applied to the keepalive interval timer in order to reduce the CPU load that may occur when multiple timers expire simultaneously.
• **holdtime**—The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0, 3 to 65,535 seconds.

**Default Configuration**
The default keepalive time is 30 seconds. The default hold time is 90 seconds.

**Command Mode**
BGP Router Configuration mode

**User Guidelines**
When BGP establishes an adjacency, the neighbors agree to use the minimum hold time configured on either neighbor. BGP sends KEEPALIVE messages at either 1/3 of the negotiated hold time or the configured keepalive interval, whichever is more frequent.

The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```bash
console(config-router)#timers bgp 1000 500
```
BGP Routing Policy

Dell EMC Networking N3000/N3100/N4000 Series Switches

Exterior routing protocols like BGP use industry-standard routing policy to filter and modify routing information exchanged with peers. BGP makes use of the following routing policy constructs:

- AS Path Access Lists
- BGP Community Lists

Use the Routing Policy commands to configure routing policies such as:

- Matching on an AS Path
- Modifying the AS Path
- Setting the local preference
- Setting the route metric
- Setting an IPv6 next hop
- Setting or matching on a BGP community

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip as-path access-list</td>
<td>show ip prefix-list</td>
</tr>
<tr>
<td>ip bgp-community new-format</td>
<td>show ipv6 prefix-list</td>
</tr>
<tr>
<td>ip community-list</td>
<td>clear ip prefix-list</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>clear ipv6 prefix-list</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>clear ip community-list</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>set as-path</td>
</tr>
<tr>
<td>match as-path</td>
<td>set comm-list delete</td>
</tr>
<tr>
<td>match community</td>
<td>set community</td>
</tr>
<tr>
<td>match ip address prefix-list</td>
<td>set ipv6 next-hop (BGP)</td>
</tr>
<tr>
<td>match ipv6 address prefix-list</td>
<td>set local-preference</td>
</tr>
<tr>
<td>show ip as-path-access-list</td>
<td>set metric</td>
</tr>
</tbody>
</table>
To create an AS path access list, use the `ip as-path access-list`. An AS path access list filters BGP routes on the AS path attribute of a BGP route. To delete an AS path access list, use the `no` form of this command.

**Syntax**

```
ip as-path access-list as-path-list-number { permit | deny } regexp
no ip as-path access-list as-path-list-number
```

- `as-path-list-number`—A number from 1 to 500 uniquely identifying the list. All AS path access list commands with the same `as-path-list-number` are considered part of the same list.
- `permit`—(Optional) Permit routes whose AS Path attribute matches the regular expression.
- `deny`—(Optional) Deny routes whose AS Path attribute matches the regular expression.
- `regexp`—A regular expression used to match the AS path attribute of a BGP path where the AS path is treated as an ASCII string.

**Default Configuration**

No AS path lists are configured by default. There are no default values for any of the parameters of this command.

**Command Mode**

Global Configuration

**User Guidelines**

The AS path attribute is a list of the autonomous system numbers along the path to the destination. An AS path access list is an ordered sequence of statements. Each statement specifies a regular expression and a permit or deny action. If the regular expression matches the AS path of the route expressed as an ASCII string, the route is considered a match and the
An AS path list has an implicit deny statement at the end. If a path does not match any of the statements in an AS path list, the action is considered to be deny.

Once you have created an AS path list, you cannot delete an individual statement. If you want to remove an individual statement, you must delete the AS path list and recreate it without the statement to be deleted.

Statements are applied in the order in which they are created. New statements are added to the end of the list. The statement with the first matching regular expression is applied.

N3000/N3100/N4000 Series switches allow configuration of up to 128 AS path access lists, with up to 64 statements each.

To enter the question mark within a regular expression, you must first enter CTRL-V to prevent the CLI from interpreting the question mark as a request for help.

<table>
<thead>
<tr>
<th><strong>Special Character</strong></th>
<th><strong>Symbol</strong></th>
<th><strong>Behavior</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>asterisk</td>
<td>*</td>
<td>Matches zero or more sequences of the pattern.</td>
</tr>
<tr>
<td>brackets</td>
<td>[ ]</td>
<td>Designates a range of single-character patterns.</td>
</tr>
<tr>
<td>caret</td>
<td>^</td>
<td>Matches the beginning of the input string.</td>
</tr>
<tr>
<td>dollar sign</td>
<td>$</td>
<td>Matches the end of the input string.</td>
</tr>
<tr>
<td>hyphen</td>
<td>–</td>
<td>Separates the end points of a range.</td>
</tr>
<tr>
<td>period</td>
<td>.</td>
<td>Matches any single character, including white space.</td>
</tr>
<tr>
<td>plus sign</td>
<td>+</td>
<td>Matches 1 or more sequences of the pattern.</td>
</tr>
<tr>
<td>question mark</td>
<td>?</td>
<td>Matches 0 or 1 occurrences of the pattern.</td>
</tr>
<tr>
<td>underscore</td>
<td>_</td>
<td>Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.</td>
</tr>
</tbody>
</table>
Example

In the following example, the router is configured to reject routes received from neighbor 172.20.1.1 with an AS path that indicates the route originates in or passes through AS 100.

```
console(config)# ip as-path access-list 1 deny _100_
console(config)# ip as-path access-list 1 deny ^100$
console(config)# router bgp 1
console(config-router)# neighbor 172.20.1.1 remote-as 200
console(config-router)# neighbor 172.20.1.1 filter-list 1 in
```

ip bgp-community new-format

To display BGP standard communities in AA:NN format, use the `ip bgp-community new-format` command. To display BGP standard communities as 32-bit integers, use the `no` form of this command.

Syntax

```
ip bgp-community new-format
no ip bgp-community new-format
```

Default Configuration

Standard communities are displayed in AA:NN format.

Command Mode

Global Configuration

User Guidelines

RFC 1997 specifies that the first two bytes of a community number are considered to be an autonomous system number. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

Example

```
console(config)#ip bgp-community new-format
```
ip community-list

To create or configure a BGP community list, use the `ip community-list` command in global configuration mode. To delete a community list, use the `no` form of this command.

Syntax

```
ip community-list standard list-name {permit | deny} [community-number] [no-advertise] [no-export] [no-export-subconfed] [no-peer]
oip community-list standard list-name
```

- **standard** list-name—Identifies a named standard community list. The name may contain up to 32 characters.
- **permit**—Indicates that matching routes are permitted.
- **deny**—Indicates that matching routes are denied.
- **community-number**—From zero to sixteen community numbers formatted as a 32-bit integers or in AA:NN format, where AA is a 2-byte autonomous system number and NN is a 16 bit integer. The range is 1 to 4,294,967,295 (any 32-bit integer other than 0). Communities are separated by spaces.
- **no-advertise**—The well-known standard community: NO_ADVERTISE (0xFFFFFF02), which indicates the community is not to be advertised.
- **no-export**—The well-known standard community: NO_EXPORT, (0xFFFFFF01), which indicates the routes are not to be advertised outside the community.
- **no-export-subconfed**—The well-known standard community: NO_EXPORT_SUBCONFED (0xFFFFFF03), which indicates the routes are not to be advertised to external BGP peers.

Default Configuration

No community lists are configured by default.

Command Mode

Global Configuration
User Guidelines

A community list statement with no community values is considered a match for all routes, regardless of their community membership. So the statement `ip community-list bullseye permit` is a permit all statement.

A community number may be entered in either format, as a 32-bit integer or a pair of 16-bit integers separated by a colon, regardless of whether the `ip bgp-community new-format` command is active. Up to 16 communities, including the well-known communities, can be listed in a single command. Up to 32 statements may be configured with a given community list name. Up to 128 unique community list names may be configured.

Example

```
console(config)#ip community-list test permit
```

**ip prefix-list**

To create a prefix list or add a prefix list entry, use the `ip prefix-list` command in global configuration mode. To delete a prefix list or a statement in a prefix list, use the `no` form of this command.

**Syntax**

```
ip prefix-list list-name {[seq number] { permit | deny } network mask [ge length] [le length] | renumber renumber-interval first-statement-number }

no ip prefix-list list-name  [seq number] { permit | deny } network mask [ge length] [le length]
```

- **list-name**—The text name of the prefix list. Up to 32 characters.
- **seq number**—(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and processed in that order. If a sequence number is not specified, the system automatically selects a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 – 4,294,967,294.
- **permit**—Permit routes whose destination prefix matches the statement.
- **deny**—Deny routes whose destination prefix matches the statement.
• network mask—Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The mask is any IPv4 prefix in dotted-quad notation.

• ge length—(Optional) If this option is configured, a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.

• le length—(Optional) If this option is configured, a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.

• renumber—Option to renumber the sequence numbers of the `ip prefix list` statements with a given interval starting from a particular sequence number.

Default Configuration

No prefix lists are configured by default. When neither the `ge` nor the `le` option is configured, the destination prefix must match the network/length exactly. If the `ge` option is configured without the `le` option, any prefix with a network mask greater than or equal to the `ge` value is considered a match. Similarly, if the `le` option is configured without the `ge` option, a prefix with a network mask less than or equal to the `le` value is considered a match.

Command Mode

Global Configuration

User Guidelines

Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route’s prefix matches that of the entry. An empty or non-existent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route’s prefix using the `match ip address` command.
The command **no ip prefix-list** list-name deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0 /16 and 192.168.1.0 /24:

```plaintext
console(config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
console(config)# ip prefix-list apple seq 20 permit 192.168.10 0.0.0.255
```

The following example disallows only the default route.

```plaintext
console(config)# ip prefix-list orange deny 0.0.0.0/0
console(config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
```

**ip prefix-list description**

To apply a text description to a prefix list, use the **ip prefix-list description** command in global configuration mode. To remove the text description, use the **no** form of this command.

**Syntax**

```
ip prefix-list list-name description text
no ip prefix-list list-name description
```

- **list-name**—The text name of the prefix list.
- **text**—Text description of the prefix list. Up to 80 characters

**Default Configuration**

No description is configured by default.
Command Mode
Global Configuration

User Guidelines
There are no user guidelines for this command.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config)#ip prefix-list test description test prefix lists

ipv6 prefix-list
To create an IPv6 prefix list or add an IPv6 prefix list entry, use the ipv6
prefix-list command in global configuration mode. To delete a prefix list or a
statement in a prefix list, use the no form of this command.

Syntax
ipv6 prefix-list list-name { seq seq-number} {permit|deny} ipv6-
prefix/prefix-length [ge ge-value] [le le-value] | description text | renumber
renumber-interval first-statement-number }

no ipv6 prefix-list list-name

• list-name—The text name of the prefix list. Up to 32 characters.
• seq number—(Optional) The sequence number for this prefix list
statement. Prefix list statements are ordered from lowest sequence number
to highest and applied in that order. If you do not specify a sequence
number, the system automatically selects a sequence number five larger
than the last sequence number in the list. Two statements may not be
configured with the same sequence number. The sequence number ranges
from 1 – 4,294,967,294.
• permit—Permit routes whose destination prefix matches the statement.
• deny—Deny routes whose destination prefix matches the statement.
- **ipv6-prefix**—The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

- **prefix-length**—The length of the IPv6 prefix given as part of the ipv6-prefix. Required if a prefix is specified. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.

- **ge length**—(Optional) Specifies a prefix length greater than or equal to the ipv6-prefix /prefix-length arguments. It is the lowest value of a range of the length (the “from” portion of the length range).

- **le length**—(Optional) Specifies a prefix length less than or equal to the ipv6-prefix /prefix-length arguments. It is the highest value of a range of the length (the “to” portion of the length range).

- **description** text—A description of the prefix list that can be up to 80 characters in length.

- **renumber-interval**—Option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval. The sequence is renumbered with the statements separated by the interval value. The renumber value ranges from 1 – 4,294,967,294.

- **first-statement-number**—Option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from the specified sequence number. The sequence is renumbered with the statements separated by the interval value beginning with the first entry with a sequence number greater than or equal to the specified value. The sequence number ranges from 1 – 4,294,967,294.

**Default Configuration**

No prefix lists are configured by default.

**Command Mode**

Global Configuration
**User Guidelines**

The `ipv6 prefix-list` command is used to create IPv6 prefix lists. These are similar to `ip prefix lists` except that the lists are IPv6 specific. An IPv6 prefix list can contain only IPv6 addresses.

Prefix lists allow matching of route prefixes against those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by sequence numbers. A router examines each prefix list entry in sequential order to determine if the route’s prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or non-existent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match occurs the router does not perform matching on the rest of the list.

An IPv6 prefix list may be used within a route map to match a route’s prefix using the match ipv6 address command. A route map may contain both IPv4 and IPv4 prefix lists. If the route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

When neither the `ge` nor the `le` option is configured, the destination prefix must match the ipv6-prefix/prefix-length exactly. If the `ge` option is configured without the `le` option, any prefix with a ipv6-prefix greater than or equal to the `ge` value is considered a match. Similarly, if the `le` option is configured without the `ge` option, a prefix with a network mask less than or equal to the `le` value is considered a match. No description is configured by default for an IPv6 prefix list.

The command `no ipv6 prefix-list list-name` deletes the entire prefix list. To remove an individual statement from a prefix list, specify the statement exactly, with all its options.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

**Command History**

Introduced in version 6.2.0.1 firmware.
Example

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 2001::/64 and 5F00::/48:

```
console(config)# ipv6 prefix-list apple seq 10 permit 2001:: /64
console(config)# ipv6 prefix-list apple seq 20 permit 5F00:: FFFF:FFFF:FFFF::
```

The following example renumbers the apple prefix list beginning at sequence number 10.

```
console(config)# ipv6 prefix-list apple renumber 10
```

match as-path

Use this command to add criteria that matches BGP autonomous system paths against an AS path access list to a route map. Use the no form of the command to remove the matching criteria from the route map.

**Syntax**

```
match as-path as-path-list-number
no match as-path as-path-list-number
```

- **as-path** as-path-list-number—An integer from 1 to 500 identifying the AS path access list to use as match criteria.

**Default Configuration**

No as-path match criteria are configured by default.

**Command Mode**

Route Map Configuration

**User Guidelines**

If a new match as-path statement is entered in a route map statement that already has a match as-path statement, the AS path list numbers in the new statement are added to the existing match term, up to the maximum number of lists in a statement. A route is considered a match if it matches any one or more of the AS path access lists to which the statement refers.
Command History
Introduced in version 6.2.0.1 firmware.

Example
console(route-map)#match as-path 250

match community
To configure a route map to match based on a BGP community list, use the match community command. To delete a match term from a route map, use the no form of this command.

Syntax
match community community-list [ community-list...] [exact-match]
no match community [ community-list [ community-list...] [exact-match] ]

- community-list—The name of a standard community list. Up to eight names may be included in a single match term.
- exact-match—(Optional) When this option is given, a route is only considered a match if the set of communities on the route is an exact match for the set of communities in one of the statements in the community list.

Default Configuration
No community match criteria are configured by default.

Command Mode
Route Map Configuration

User Guidelines
If the community list returns a permit action, the route is considered a match. If the match statement refers to a community list that is not configured, no routes are considered to match the statement.

no match community list exact-match removes the match statement from the route map. (It doesn’t simply remove the exact-match option.)
The command `no match community` removes the match term and all its community lists.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```bash
console(route-map)#match community test
```

### match ip address prefix-list

Use this command to configure a route map to match based on a destination prefix. To delete a match statement from a route map, use the `no` form of this command.

**Syntax**

```bash
match ip address prefix-list prefix-list-name [prefix-list-name...]
no match ip address prefix-list [prefix-list-name [prefix-list-name...]]
```

- `prefix-list` prefix-list-name—The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

**Default Configuration**

No match criteria are configured by default.

**Command Mode**

Route Map Configuration

**User Guidelines**

If multiple prefix lists are specified in one statement, a match occurs if a prefix matches any one of the prefix lists. If a `match ip address` statement is configured within a route map section that already has a `match ip address` statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

The command `no match ip address prefix-list` removes the match term and all its prefix lists.
Command History
Introduced in version 6.2.0.1 firmware.

Example
console(route-map)#match ip address prefix-list test

match ipv6 address prefix-list
Use this command to configure a route map to match based on an IPv6
destination prefix. To delete a match statement from a route map, use the no form of this command.

Syntax
match ip address prefix-list prefix-list-name [prefix-list-name...]
no match ip address prefix-list [ prefix-list-name [prefix-list-name...] ]

• prefix-list prefix-list-name—The name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

Default Configuration
No match criteria are configured by default.

Command Mode
Route Map Configuration

User Guidelines
If multiple prefix lists are specified in one statement, a match occurs if a prefix matches any one of the prefix lists. If a match ipv6 address statement is configured within a route map section that already has a match ipv6 address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.
The command no match ip address prefix-list removes the match term and all its prefix lists.
Command History
Introduced in version 6.2.0.1 firmware.

Example
In the example below, IPv6 addresses specified by the prefix list apple are matched through the route map abc.

Router(config)# route-map abc
Router(config-route-map)# match ipv6 address prefix-list apple

show ip as-path-access-list
This command displays the contents of AS path access lists.

Syntax
show ip as-path-access-list [ as-path-list-number ]
- as-path-list-number—(Optional) When an AS path list number is specified, the output is limited to the single AS path list specified. Integer from 1 to 500.

Default Configuration
No match criteria are configured by default.

Command Mode
Privileged Exec mode, Global Configuration mode and all sub-modes.

User Guidelines
There are no user guidelines for this command.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console#show ip as-path-access-list

AS path access list 1
deny _100_
deny ^100$
show ip community-list

This command displays the contents of AS path access lists.

Syntax

show ip community-list [community-list-name | detail [community-list-name]]

- community-list-name—(Optional) A standard community list name. This option limits the output to a single community.
- detail—Display detailed community list information

Default Configuration

No match criteria are configured by default.

Command Mode

Privileged Exec mode, Global Configuration mode and all sub-modes.

User Guidelines

There are no user guidelines for this command.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console#show ip community-list

Standard community list buzz
    permit 100:200
    permit 100:300
    permit 100:400
Standard community list woody
    permit 200:1
    permit 200:2
    permit 200:3
**show ip prefix-list**

This command displays the contents of IPv4 prefix lists.

**Syntax**

```
show ip prefix-list [detail [prefix-list-name] | summary [prefix-list-name] | prefix-list-name [network mask [longer] [first-match] | seq sequence-number]] [detail | summary] prefix-list-name [network network-mask] [seq sequence-number] [longer] [first-match]
```

- **detail | summary**—(Optional) Displays detailed or summarized information about all prefix lists.
- **prefix-list-name**—(Optional) The name of a specific prefix list.
- **network**—(Optional) The network number
- **mask**—Required if a network is specified. The network mask dotted-quad notation. In dotted-quad notation, the 1 bits must be contiguous and left justified.
- **seq sequence-number**—(Optional) Applies the sequence number to the prefix list entry. The sequence number of the prefix list entry.
- **longer**—(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
- **first-match**—(Optional) Displays the entry of a prefix list that matches the given network.

**Default Configuration**

No prefix lists are configured by default.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**

The following combinations of parameters are acceptable:

```
show ip prefix-list prefix-list-name network /length first-match
show ip prefix-list prefix-list-name network /length longer
show ip prefix-list prefix-list-name network /length
```
show ip prefix-list prefix-list-name seq sequence-number
show ip prefix-list prefix-list-name
show ip prefix-list summary
show ip prefix-list summary prefix-list-name
show ip prefix-list detail
show ip prefix-list detail prefix-list-name
show ip prefix-list
The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number of entries in the prefix list.</td>
</tr>
<tr>
<td>range entries</td>
<td>Number of entries that match the input range.</td>
</tr>
<tr>
<td>ref count</td>
<td>Number of entries referencing the given prefix list.</td>
</tr>
<tr>
<td>seq</td>
<td>Sequence number of the entry in the list.</td>
</tr>
<tr>
<td>permit/deny</td>
<td>Actions.</td>
</tr>
<tr>
<td>sequences</td>
<td>Range of sequence numbers for the entries in the list.</td>
</tr>
<tr>
<td>hit count</td>
<td>Number of times the prefix was matched in the routing decision process.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```console
console#show ip prefix-list fred
ip prefix-list fred:
    count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
    seq 5 permit 10.10.1.1/20 ge 22
    seq 10 permit 10.10.1.2/20 le 30
    seq 15 permit 10.10.1.2/20 ge 29 le 30

console#show ip prefix-list summary fred
ip prefix-list fred:
    count: 3, range entries: 3, sequences: 5 - 15, refcount: 0

console#show ip prefix-list detail fred
```
show ipv6 prefix-list

This command displays the contents of IPv6 prefix lists.

Syntax

show ipv6 prefix-list [detail [prefix-list-name] | summary [prefix-list-name] | prefix-list-name [ipv6-prefix/prefix-length [longer] [first-match] | seq sequence-number ]]

• detail | summary – (Optional) Displays detailed or summarized information about all prefix lists.
• prefix-list-name – (Optional) The name of a specific prefix list. Information is limited to this particular prefix list.
• ipv6-prefix - An IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons.
• prefix-length - The length of the IPv6 prefix given as part of the ipv6-prefix. Required if a prefix is specified. A decimal value in the range 0 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.
• seq – (Optional) Applies the sequence number to the prefix list entry.
• sequence-number – (Optional) The sequence number of the prefix list entry.
• longer – (Optional) Displays all entries of a prefix list that are more specific than the given network/length.
• first-match – (Optional) Displays the entry of a prefix list that matches the given prefix /prefix-length.
**Default Configuration**
No prefix lists are configured by default.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**
The following information is displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number of entries in the prefix list.</td>
</tr>
<tr>
<td>range entries</td>
<td>Number of entries that match the input range.</td>
</tr>
<tr>
<td>ref count</td>
<td>Number of entries referencing the given prefix list.</td>
</tr>
<tr>
<td>seq</td>
<td>Sequence number of the entry in the list.</td>
</tr>
<tr>
<td>permit/deny</td>
<td>Actions.</td>
</tr>
<tr>
<td>sequences</td>
<td>Range of sequence numbers for the entries in the list.</td>
</tr>
<tr>
<td>hit count</td>
<td>Number of times the prefix was matched in the routing decision process.</td>
</tr>
</tbody>
</table>

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**

```console
console# show ipv6 prefix-list apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
  seq 5 deny 5F00::/8 le 128
  seq 10 deny ::/0
  seq 15 deny ::/1
  seq 20 deny ::/2
  seq 25 deny ::/3 ge 4
  seq 30 permit ::/0 le 128

console# show ipv6 prefix-list summary apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31

console# show ipv6 prefix-list detail apple
```
Layer 3 Routing Commands

ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
seq 10 deny ::/0 (hit count: 0, refcount: 1)
seq 15 deny ::/1 (hit count: 0, refcount: 1)
seq 20 deny ::/2 (hit count: 0, refcount: 1)
seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)

**clear ip prefix-list**

To reset the IPv4 prefix-list counters, use the clear ip prefix-list command.

**Syntax**

```
clear ip prefix-list [list-name | list-name network mask]
```

- **list-name**—(Optional) Name of the prefix list from which the hit count is to be cleared.
- **network**— (Optional) Network number. If this option is specified, hit counters are cleared only for the matching prefixes.
- **mask**—Required if a network is specified. The network mask in dotted-quad notation. In dotted-quad notation, the 1 bits must be contiguous and left justified.

**Default Configuration**

No prefix lists are configured by default.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**

This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry. The counters are also cleared by the global clear counters command.

**Command History**

Introduced in version 6.2.0.1 firmware.
Example

console# clear ip prefix-list orange 20.0.0.0 /8

clear ipv6 prefix-list

To reset the IPv6 prefix-list counters, use the clear ipv6 prefix-list command.

Syntax

clear ipv6 prefix-list [list-name | list-name ipv6-prefix/prefix-length]

- list-name – (Optional) Name of the IPv6 prefix list from which the hit count is to be cleared.
- ipv6-prefix - An IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between 0x00 and 0xff and separated by colons. Counters are cleared only for the matching prefixes.
- prefix-length - The length of the IPv6 prefix given as part of the ipv6-prefix. Required if a prefix is specified. A decimal value in the range 0 to 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) in /length format. A slash mark must precede the decimal value in /length format.

Default Configuration

No prefix lists are configured by default.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

User Guidelines

This command is used to clear the IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry. The counters are also cleared by the global clear counters command.

Command History

Introduced in version 6.2.0.1 firmware.
Example
The command below clears the counters only for the matching statement in the IPv6 prefix list apple.

```
Router# clear ipv6 prefix-list apple FF05::/35
```

**clear ip community-list**

To reset the IPv6 prefix-list counters, use the clear ipv6 prefix-list command.

**Syntax**

clear ip community-list [list-name]

- list-name—(Optional) Name of the community list for which the hit count is to be cleared.

**Default Configuration**

No community lists are configured by default.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command is used to clear the community list hit counters. The hit count is a value indicating the number of matches to a specific list entry. The counters are also cleared by the global clear counters command.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

The command below clears the counters only for the matching community apple.

```
Router# clear ip community-list apple
```
**set as-path**

To prepend one or more AS numbers to the AS path in a BGP route, use the `set as-path` command. To remove a set command from a route map, use the `no` form of this command.

**Syntax**

```plaintext
set as-path prepend as-path-string
no set as-path prepend as-path-string
```

- `prepend as-path-string`—A list of AS path numbers to insert at the beginning of the AS_PATH attribute of matching BGP routes. To prepend more than one AS number, separate the ASNs with a space and enclose the string in quotes. Up to ten AS numbers may be prepended.

**Default Configuration**

No AS paths are prepending by default.

**Command Mode**

Route Configuration

**User Guidelines**

This command is normally used to insert one or more instances of the local AS number at the beginning of the AS_PATH attribute of a BGP route. Doing so increases the AS path length of the route. The AS path length has a strong influence on BGP route selection. Changing the AS path length can influence route selection on the local router or on routers to which the route is advertised.

When prepending an inbound route, if the first segment in the AS_PATH of the received route is an AS_SEQUENCE, `as-path-string` is inserted at the beginning of the sequence. If the first segment is an AS_SET, `as-path-string` is added as a new segment with type AS_SEQUENCE at the beginning of the AS path. When prepending an outbound route to an external peer, `as-path-string` follows the local AS number, which is always the first ASN.

**Command History**

Introduced in version 6.2.0.1 firmware.
Example

```console
console# config
console(config)#route-map ppAsPath
console(route-map)#set as-path prepend “2 2 2”
console(route-map)#exit
console(config)#router bgp 1
console(config-rtr)#neighbor 172.20.1.2 remote-as 2
console(config-rtr)#neighbor 172.20.1.2 route-map ppAsPath in
```

**set comm-list delete**

To remove BGP communities from an inbound or outbound UPDATE message, use the `set comm-list delete` command. To delete the set command from a route map, use the `no` form of this command.

**Syntax**

```
set comm-list community-list-name delete
no set comm-list
```

- community-list-name—A standard community list name.

**Default Configuration**

No communities are removed from UPDATE messages by default.

**Command Mode**

Route Map Configuration

**User Guidelines**

A route map with this set command can be used to remove selected communities from inbound and outbound routes. When a community list is applied to a route for this purpose, each of the route’s communities is submitted to the community list one at a time. Communities permitted by the list are removed from the route. Since communities are processed individually, a community list used to remove communities should not include the `exact-match` option on statements with multiple communities. Such statements can never match an individual community.
When a route map statement includes both set community and set comm-list delete terms, the set comm-list delete term is processed first, and then the set community term (that is, communities are first removed, and then communities are added).

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
console(route-map)#set comm-list test delete

**set community**
To modify the communities attribute of matching routes, use the set community command in route-map configuration mode. To remove a set term from a route map, use the no form of this command

**Syntax**

```
set community {{community-number | no-export | no-advertise} no set community
```

- **community-number**—One to sixteen community numbers, either as a 32-bit integers or in AA:NN format. Communities are separated by spaces. The well-known communities no-advertise and no-export are also accepted.

- **no-advertise**—The well-known standard community: NO_ADVERTISE (0xFFFFFF02) which indicates the community is not to be advertised.

- **no-export**—The well-known standard community: NO_EXPORT, (0xFFFFFF01), which indicates the routes are not to be advertised outside the community.

- **additive**—(Optional) Communities are added to those already attached to the route.

- **none**—(Optional) Removes all communities from matching routes.

**Default Configuration**
No communities are set by default.
**Command Mode**
Route Map Configuration

**User Guidelines**
The `set community` command can be used to assign communities to routes originated through BGP’s network and redistribute commands and to set communities on routes received from a specific neighbor or advertised to a specific neighbor. It can also be used to remove all communities from a route. To remove a subset of the communities on a route, use the `set comm-list delete` command.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(route-map)#set community no-advertise
```

### set ipv6 next-hop (BGP)
To set the IPv6 next hop of a route, use the `set ipv6 next-hop` command in route-map configuration mode. To remove a set command from a route map, use the no form of this command.

**Syntax**
```
set ipv6 next-hop ipv6-address
no set ipv6 next-hop
```

- ipv6-address—The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

**Default Configuration**
No next-hops are set by default.

**Command Mode**
Route Map Configuration
User Guidelines
When used in a route map applied to UPDATE messages received from a neighbor, the command sets the next hop address for matching IPv6 routes received from the neighbor. When used in a route map applied to UPDATE messages sent to a neighbor, the command sets the next hop address for matching IPv6 routes sent to the neighbor. If the address is a link local address, the address is assumed to be on the interface where the UPDATE is sent or received. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

Command History
Introduced in version 6.2.0.1 firmware.

Example
```
console(route-map)#set ipv6 next-hop FE80::0202:B3FF:FE1E:8329
```

**set local-preference**

To set the local preference of specific BGP routes, use the `set local-preference` command in route-map configuration mode. To remove a set command from a route map, use the `no` form of this command.

**Syntax**
```
set local-preference value
no set local-preference value
```

- **value**—A local preference value, from 0 to 4,294,967,295 (any 32 bit integer).

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Route Map Configuration
**User Guidelines**

The local preference is the first attribute used to compare BGP routes. Setting the local preference can influence which route BGP selects as the best route. When used in conjunction with a `match as-path` or `match ip-address` command, this command can be used to prefer routes that transit certain ASs or to make the local router a more preferred exit point to certain destinations.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(route-map)#set local-preference 6432
```

**set metric**

To set the metric of a route, use the `set metric` command. To remove a set command from a route map, use the `no` form of this command.

**Syntax**

```
set metric value
no set metric value
```

- **value**—A local preference value, from 0 to 4,294,967,295 (any 32 bit integer).

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Route Map Configuration

**User Guidelines**

This command sets the Multi Exit Discriminator (MED) when used in a BGP context. When there are multiple peering points between two autonomous systems (AS), setting the MED on routes advertised by one router can influence the other AS to send traffic through a specific peer.
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(route-map)#set metric 6432
```
Distance Vector Multicast Routing Protocol (DVMRP) is a dense mode multicast protocol and is most appropriate for use in networks where bandwidth is relatively plentiful and there is at least one multicast group member in each subnet. DVMRP assumes that all hosts are part of a multicast group until it is informed of multicast group changes. When the dense-mode multicast router is informed of a group membership change, the multicast delivery tree is pruned. DVMRP uses a distributed routing algorithm to build per-source-group multicast trees. It is also called Broadcast and Prune Multicasting protocol. It dynamically generates per-source-group multicast trees using Reverse Path Multicasting. Trees are calculated and updated dynamically to track membership of individual groups.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dvmrp</td>
<td>Use the command to set the administrative mode of DVMRP in the router to active. Enabling DVMRP concurrently enables IGMP/MLD. Using the no form of the command sets the administrative mode to inactive and disables IGMP/MLD.</td>
</tr>
<tr>
<td>show ip dvmrp neighbor</td>
<td></td>
</tr>
<tr>
<td>show ip dvmrp nexthop</td>
<td></td>
</tr>
<tr>
<td>show ip dvmrp prune</td>
<td></td>
</tr>
<tr>
<td>show ip dvmrp route</td>
<td></td>
</tr>
</tbody>
</table>

**ip dvmrp**

Use the **ip dvmrp** command to set the administrative mode of DVMRP in the router to active. Enabling DVMRP concurrently enables IGMP/MLD. Using the no form of the command sets the administrative mode to inactive and disables IGMP/MLD.

**Syntax**

```
ip dvmrp
no ip dvmrp
```
**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Global Configuration
Interface Configuration (VLAN) mode

**User Guidelines**

PIM must be disabled before DVMRP can be enabled. This command enables IGMP/MLD. Disabling IGMP/MLD may operationally disable multicast routing.

**Example**

The following example sets VLAN 15’s administrative mode of DVMRP to active.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip dvmrp
```

**ip dvmrp metric**

Use the `ip dvmrp metric` command in Interface Configuration mode to configure the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network.

**Syntax**

```
ip dvmrp metric metric
no ip dvmrp metric
```

- **metric** — Cost to reach the network. (Range: 1-31)

**Default Configuration**

1 the default value.

**Command Mode**

Interface Configuration (VLAN) mode
**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures a metric of 5 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip dvmrp metric 5
```

**show ip dvmrp**
Use the `show ip dvmrp` command to display the system-wide information for DVMRP.

**Syntax**
```
show ip dvmrp
```

**Default Configuration**
This command has no default condition.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays system-wide information for DVMRP.

```
console(config)#show ip dvmrp
Admin Mode.................................. Enabled
Version...................................... 3
Total Number of Routes..................... 0
Reachable Routes........................... 0

   DVMRP INTERFACE STATUS

Interface  Interface Mode  Operational-Status
---------  --------------  ------------------
**show ip dvmrp interface**

Use the `show ip dvmrp interface` command to display the interface information for DVMRP on the specified interface.

**Syntax**

`show ip dvmrp interface vlan vlan-id`

- `vlan-id` — Valid VLAN ID.

**Default Configuration**

This command has no default condition.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays interface information for VLAN 11 DVMRP.

```
console(config)#show ip dvmrp interface vlan 11
Interface Mode................................ Enabled
Interface Metric................................ 5
Local Address.................................. 10.1.0.2
Received Bad Packets........................... 0
Received Bad Routes............................ 0
Sent Routes.................................... 0
```

**show ip dvmrp neighbor**

Use the `show ip dvmrp neighbor` command to display the neighbor information for DVMRP.

**Syntax**

`show ip dvmrp neighbor`
Default Configuration
This command has no default condition.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the neighbor information for DVMRP.

console(config)#show ip dvmrp neighbor
No neighbors available.

show ip dvmrp nexthop
Use the show ip dvmrp nexthop command to display the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax
show ip dvmrp nexthop

Default Configuration
This command has no default condition.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.
**Example**

The following example displays the next hop information on outgoing interfaces for routing multicast datagrams.

```bash
console(config)#show ip dvmrp nexthop
```

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source Mask</th>
<th>Interface</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>------</td>
</tr>
</tbody>
</table>

**show ip dvmrp prune**

Use the `show ip dvmrp prune` command to display the table that lists the router’s upstream prune information.

**Syntax**

`show ip dvmrp prune`

**Default Configuration**

This command has no default condition.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration sub-modes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the table that lists the router’s upstream prune information.

```bash
console(config)#show ip dvmrp prune
```

<table>
<thead>
<tr>
<th>Group IP</th>
<th>Source IP</th>
<th>Source Mask</th>
<th>Expiry Time(secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.0.1.43</td>
<td>10.1.0.3</td>
<td>255.255.0.0</td>
<td>237</td>
</tr>
</tbody>
</table>
show ip dvmrp route

Use the show ip dvmrp route command to display the multicast routing information for DVMRP.

Syntax

show ip dvmrp route

Default Configuration

This command has no default.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast routing information for DVMRP.

```
console#show ip dvmrp route
console(config)#show ip dvmrp route

<table>
<thead>
<tr>
<th>Upstream</th>
<th>Source Address</th>
<th>Source Mask</th>
<th>Neighbor</th>
<th>Intf</th>
<th>Metric</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

UpTime
IGMP Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

The Dell Network N1500/N2000/N2100-ON Series switches support limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

Internet Group Management Protocol (IGMP) is the multicast group membership discovery protocol used for IPv4 multicast groups. Three versions of IGMP exist. Versions one and two are widely deployed. Since IGMP is used between end systems (often desktops) and the multicast router, the version of IGMP required depends on the end-user operating system being supported. Any implementation of IGMP must support all earlier versions.

The following list describes the basic operation of IGMP, common to all versions. A multicast router can act as both an IGMP host and an IGMP router and as a result can respond to its own IGMP messages. The Dell EMC Networking implementation of IGMPv3 supports the multicast router portion of the protocol (that is, not the host portion). It is backward compatible with IGMPv1 and IGMPv2.

- One router periodically broadcasts IGMP Query messages onto the network.
- Hosts respond to the Query messages by sending IGMP Report messages indicating their group memberships.
- All routers receive the Report messages and note the memberships of hosts on the network.
- If a router does not receive a Report message for a particular group for a period of time, the router assumes there are no more members of the group on the network.

All IGMP messages are raw IP data grams and are sent to multicast group addresses, with a time to leave (TTL) of 1. Since raw IP does not provide reliable transport, some messages are sent multiple times to aid reliability.

IGMPv3 is a major revision of the protocol and provides improved group membership latency. When a host joins a new multicast group on an interface, it immediately sends an unsolicited IGMP Report message for that group.
IGMPv2 introduced a Leave Group message, which is sent by a host when it leaves a multicast group for which it was the last host to send an IGMP Report message. Receipt of this message causes the Querier possibly to reduce the remaining lifetime of its state for the group, and to send a group-specific IGMP Query message to the multicast group. The Leave Group message is not used with IGMPv3, since the source address filtering mechanism provides the same functionality.

IGMPv3 also allows hosts to specify the list of hosts from which they want to receive traffic. Traffic from other hosts is blocked inside the network. It also allows hosts to block packets for all sources sending unwanted traffic. IGMPv3 adds the capability for a multicast router to learn which sources are of interest to neighboring systems for packets sent to any particular multicast address. This information gathered by IGMP is provided to the multicast routing protocol (that is, DVMRP, PIM-DM, and PIM-SM) that is currently active on the router in order to ensure multicast packets are delivered to all networks where there are interested receivers.

IGMP mode is automatically enabled when PIM, DVMRP, or IGMP Proxy is enabled.

**Commands in this Section**

This section explains the following commands:

- `ip igmp last-member-query-count`
- `ip igmp last-member-query-interval`
- `ip igmp mroute-proxy`
- `ip igmp query-interval`
- `ip igmp query-max-response-time`
- `ip igmp robustness`
- `ip igmp startup-query-count`
- `ip igmp startup-query-interval`
- `ip igmp version`
- `show ip igmp`
- `show ip igmp groups`
- `show ip igmp interface`
- `show ip igmp membership`
- `show ip igmp interface stats`

**ip igmp last-member-query-count**

Use the `ip igmp last-member-query-count` command in Interface Configuration mode to set the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.
**Syntax**

ip igmp last-member-query-count Imqc
no ip igmp last-member-query-count

- Imqc — Query count. (Range: 1-20)

**Default Configuration**

The default last member query count is 2.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets 10 as the number of VLAN 2 Group-Specific Queries.

```console
console#configure
console(config)#interface vlan 2
console(config-if-vlan2)#ip igmp last-member-query-count 10
console(config-if-vlan2)#no ip igmp last-member-query-count
```

**ip igmp last-member-query-interval**

Use the `ip igmp last-member-query-interval` command in Interface Configuration mode to configure the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.

**Syntax**

ip igmp last-member-query-interval tenthsofseconds
no ip igmp last-member-query-interval

- tenthsofseconds — Maximum Response Time in tenths of a second (Range: 0-255)
**Default Configuration**
The default Maximum Response Time value is ten (in tenths of a second).

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures 2 seconds as the Maximum Response Time inserted in VLAN 15’s Group-Specific Queries.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp last-member-query-interval 20
```

**ip igmp mroute-proxy**
This command configures downstream IGMP proxy on the selected VLAN interface associated with multicast hosts. Use this command to enable the proxying of IGMP messages received on the local interface to the multicast router connected interface enabled with the `ip igmp proxy-service` command.

PIM and DVMRP are not compatible with IGMP proxy. Disable PIM/DVMRP before enabling IGMP proxy.

Multicast routing must be enabled for the IGMP proxy service to become operationally enabled.

IGMP is enabled when `ip pim sparse-mode`, `ip pim dense-mode`, `ip dvmrp`, or `ip igmp-proxy` are enabled. IP multicast routing must be globally enabled and an upstream interfaces must be configured using the the `ip igmp proxy-service` command. If ip pim or ip dvmrp is enabled, this command is not displayed in the `running-config`.

**Syntax**
```
ip igmp mroute-proxy
no ip igmp mroute-proxy
```
**Default Configuration**
Disabled is the default state.

**Command Mode**
Interface VLAN Configuration mode

**User Guidelines**
IGMP is enabled when `ip pim sparse-mode`, `ip pim dense-mode`, `ip dvmrp`, or `ip igmp-proxy` are enabled.
A multicast routing protocol (e.g. PIM) should be enabled whenever IGMP is enabled.
L3 IP multicast must be enabled for IGMP to operate.

**Example**
The following example globally enables IGMP the IGMP proxy service on VLAN 1.

```plaintext
console(config)#ip multicast-routing
console(config)#interface vlan 1
console(config-if-vlan1)#ip igmp mroute-proxy
```

**ip igmp query-interval**
Use the `ip igmp query-interval` command in Interface Configuration mode to configure the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.

**Syntax**

- `ip igmp query-interval` seconds
- `no ip igmp query-interval`
  - seconds — Query interval. (Range: 1-3600)

**Default Configuration**
The default query interval value is 125 seconds.
**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures a 10-second query interval for VLAN 15.
```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp query-interval 10
```

**ip igmp query-max-response-time**
Use the `ip igmp query-max-response-time` command in Internet Configuration mode to configure the maximum response time interval for the specified interface. It is the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in seconds.

**Syntax**
```
ip igmp query-max-response-time seconds
no ip igmp query-max-response-time
```

- **seconds** — Maximum response time. (Range: 0-25 seconds)

**Default Configuration**
The default maximum response time value is 10 seconds.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures a maximum response time interval of one second for VLAN 15.
ip igmp robustness

Use the **ip igmp robustness** command in Interface VLAN Configuration mode to configure the robustness that allows tuning of the interface, that is, tuning for the expected packet loss on a subnet. If a subnet is expected to have significant loss, the robustness variable may be increased for the interface.

**Syntax**

```
ip igmp robustness robustness
no ip igmp robustness
```

- **robustness** — Robustness variable. (Range: 1-255)

**Default Configuration**

The default robustness value is 2.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures a robustness value of 10 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp robustness 10
```

**ip igmp startup-query-count**

Use the **ip igmp startup-query-count** command in Interface VLAN Configuration mode to set the number of queries sent out on startup—at intervals equal to the startup query interval for the interface.
Syntax

ip igmp startup-query-count count
no ip igmp startup-query-count

- count — The number of startup queries. (Range: 1-20)

Default Configuration

The default count value is 2.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets for VLAN 15 the number of queries sent out on startup at 10.

console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp startup-query-count 10

ip igmp startup-query-interval

Use the ip igmp startup-query-interval command in Interface Configuration mode to set the interval between general queries sent at startup on the interface.

Syntax

ip igmp startup-query-interval seconds
no ip igmp startup-query-interval

- seconds — Startup query interval. (Range: 1-300 seconds)

Default Configuration

The default interval value is 31 seconds.
**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets at 10 seconds the interval between general queries sent at startup for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp startup-query-interval 10
```

**ip igmp version**
Use the `ip igmp version` command in Interface Configuration mode to configure the version of IGMP for an interface.

**Syntax**

```
ip igmp version version
```

- version — IGMP version. (Range: 1-3)

**Default Configuration**
The default version is 3.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures version 2 of IGMP for VLAN 15.

```
console#interface vlan 15
console(config-if-vlan15)#ip igmp version 2
```
show ip igmp

Use the show ip igmp command to display system-wide IGMP information.

Syntax
show ip igmp

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays system-wide IGMP information.

console#show ip igmp

IGMP Admin Mode............................. Enabled
IGMP Router-Alert check..................... Disabled

IGMP INTERFACE STATUS
Interface Interface-Mode Operational-Status
--------- -------------- ----------------
vlan 3    Enabled        Non-Operational

show ip igmp groups

Use the show ip igmp groups command in User Exec or Privileged Exec modes to display the registered multicast groups on the interface. If detail is specified, this command displays the registered multicast groups on the interface in detail.

Syntax
show ip igmp groups [interface-type interface-number] [detail]
• interface-type interface-number—Interface type of VLAN and a valid VLAN ID

Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the registered multicast groups for VLAN 3.

csone#show ip igmp groups vlan 3 detail

<table>
<thead>
<tr>
<th>Multicast IP Address</th>
<th>Last Reporter</th>
<th>Up Time</th>
<th>Expiry Time</th>
<th>Host Timer</th>
<th>Host Timer</th>
<th>Compat Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.0.5</td>
<td>1.1.1.5</td>
<td>00:00:05</td>
<td>00:04:15</td>
<td>-----</td>
<td>00:04:15</td>
<td>v2</td>
</tr>
</tbody>
</table>

show ip igmp interface

Use the show ip igmp interface command to display the IGMP information for the specified interface.

Syntax
show ip igmp interface [stats][interface-type interface-number]

• interface-type interface-number—Interface type of VLAN and a valid VLAN ID

• stats—Displays IGMP statistics for the specified VLAN.

Default Configuration
This command has no default configuration.
**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays IGMP information for VLAN 11.

```
console#show ip igmp interface vlan 11
Interface..................................... 11
IGMP Admin Mode............................... Enable
Interface Mode................................ Enable
IGMP Version.................................. 3
Query Interval (secs)......................... 125
Query Max Response Time (1/10 of a second).... 100
Robustness..................................... 2
Startup Query Interval (secs)............... 31
Startup Query Count............................ 2
Last Member Query Interval (1/10 of a second) 10
Last Member Query Count...................... 2
```

**show ip igmp membership**
Use the `show ip igmp membership` command to display the list of interfaces that have registered in the multicast group. If `detail` is specified, this command displays detailed information about the listed interfaces.

**Syntax**

```
show ip igmp membership [groupaddr] [detail]
```

- `groupaddr` — Group IP address

**Default Configuration**
This command has no default configuration.

**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

This command has no user guidelines.

**Examples**

The following examples display the list of interfaces that have registered in the multicast group at IP address 224.5.5.5, the latter in detail mode.

```
console#show ip igmp interface membership 224.5.5.5

console(config)#show ip igmp membership 224.5.5.5 detail
```

**show ip igmp interface stats**

Use the `show ip igmp interface stats` command in User Exec mode to display the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

**Syntax**

```
show ip igmp interface stats vlan vlan-id
```

- `vlan-id` — Valid VLAN ID

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Examples**

The following example displays the IGMP statistical information for VLAN 7.

```
console#show ip igmp interface stats vlan 7
Querier Status............................... Querier
Querier IP Address............................ 7.7.7.7
Querier Up Time (secs)....................... 55372
Querier Expiry Time (secs)................... 0
Wrong Version Queries....................... 0
```
Number of Joins.............................. 7
Number of Groups............................. 1
IGMP Proxy Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

IGMP Proxy is used by the router on IPv4 systems to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces, thus acting as proxy to all its hosts residing on its router interfaces.


Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp proxy-service</td>
<td>Use the ip igmp proxy-service command in Interface Configuration mode to enable the IGMP Proxy on the VLAN interface. Use this command to enable the sending of IGMP messages received on interfaces configured with the ip igmp mroute-proxy command to an attached multicast router. IGMP is enabled with IGMP proxy. Only one interface can be configured with the IGMP proxy service. This interface forwards IGMP reports to a multicast router on behalf of IGMP clients configured with the ip igmp mroute-proxy command.</td>
</tr>
</tbody>
</table>

Syntax

ip igmp proxy-service
no ip igmp proxy-service

**Default Configuration**
Disabled is the default configuration.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command enables IGMP proxy on the VLAN interface. Use this command to enable sending of IGMP messages received on interfaces configured with the `ip igmp mroute-proxy` command to an attached multicast router.

PIM and DVMRP are not compatible with IGMP proxy. Disable PIM/DVMRP before enabling IGMP proxy.

Multicast routing must be enabled for the IGMP proxy service to become operationally enabled. This command enables IGMP/MLD. Disabling IGMP Proxy may operationally disable multicast routing.

**Example**
The following example enables the IGMP Proxy on the VLAN 15 router.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy
```

**ip igmp proxy-service reset-status**
Use the `ip igmp proxy-service reset-status` command in Interface Configuration mode to reset the host interface status parameters of the IGMP Proxy router. This command is valid only when IGMP Proxy is enabled on the interface.

**Syntax**
```
ip igmp proxy-service reset-status
```

**Default Configuration**
This command has no default configuration.
**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example resets the host interface status parameters of the IGMP Proxy router.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp proxy-service reset-status
```

### ip igmp proxy-service unsolicit-rprt-interval

Use the `ip igmp proxy-service unsolicit-rprt-interval` command in Interface Configuration mode to set the unsolicited report interval for the IGMP Proxy router. This command is valid only if IGMP Proxy on the interface is enabled.

**Syntax**
```
ip igmp proxy-service unsolicit-rprt-interval seconds
```
- `seconds` — Unsolicited report interval. (Range: 1-260 seconds)

**Default Configuration**
The default configuration is 1 second.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets 10 seconds as the unsolicited report interval for the IGMP Proxy router.

```console
console(config)#interface vlan 15
```
show ip igmp proxy-service

Use the `show ip igmp proxy-service` command to display a summary of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

**Syntax**

`show ip igmp proxy-service`

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays a summary of the host interface status parameters.

```plaintext
console#show ip igmp proxy-service
Interface Index............................... vlan13
Admin Mode.................................... Enable
Operational Mode.............................. Enable
Version....................................... 3
Number of Multicast Groups.................... 0
Unsolicited Report Interval................... 1
Querier IP Address on Proxy Interface........ 0.0.0.0
Older Version 1 Querier Timeout............. 0
Older Version 2 Querier Timeout............. 0
Proxy Start Frequency....................... 1
```
**show ip igmp proxy-service interface**

Use the **show ip igmp proxy-service interface** command to display a detailed list of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

**Syntax**

```
show ip igmp proxy-service interface
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example fails to display status parameters because IGMP Proxy is not enabled.

```
console#show ip igmp proxy-service interface
Interface Index......................... vlan13
Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-------------------------------
1         0            0            0        -----       ----- 
2         0            0            0          0           0 
3         0            0            0        -----       ----- 
```

**show ip igmp-proxy groups**

Use the **show ip igmp proxy-service groups** command to display a table of information about multicast groups that IGMP Proxy reported. It displays status parameters only when IGMP Proxy is enabled.

**Syntax**

```
show ip igmp proxy-service groups
```

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example attempts to display a table of information about multicast groups that IGMP Proxy reported.

```
console#show ip igmp proxy-service groups
Interface Index.................. vlan13
Group Address  Last Reporter    Up Time   Member State Filter Mode Sources
-------------  ---------------  -------   ------------ ----------- ------
225.0.1.1        13.13.13.1     7         DELAY-MEMBER Exclude       0
225.0.1.2        13.13.13.1    48         DELAY-MEMBER Exclude       0
```

```
show ip igmp proxy-service groups detail

Use the `show ip igmp proxy-service groups detail` command to display complete information about multicast groups that IGMP Proxy has reported.

Syntax
show ip igmp proxy-service groups detail

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays complete information about multicast groups that IGMP Proxy has reported.

```console
console#show ip igmp proxy-service groups detail
Interface Index.......................... vlan13

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Last Reporter</th>
<th>Up Time</th>
<th>Member State</th>
<th>Filter Mode</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.1</td>
<td>13.13.13.1</td>
<td>26</td>
<td>DELAY-MEMBER</td>
<td>Exclude</td>
<td>0</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>13.13.13.1</td>
<td>67</td>
<td>DELAY-MEMBER</td>
<td>Exclude</td>
<td>0</td>
</tr>
</tbody>
</table>
```
IP Helper/DHCP Relay Commands

Dell EMC Networking N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The IP Helper feature provides the ability for a router to forward configured UDP broadcast packets to a particular IP address over a routed interface. This allows applications to reach servers on non-local subnets. This is possible even when the application is designed to assume a server is always on a local subnet or when the application uses broadcast packets to reach the server (using the broadcast MAC address FF:FF:FF:FF:FF:FF and with the IP broadcast address 255.255.255.255 or a network directed broadcast IP address on the receiving switch interface). IP routing must be enabled for IP Helper to forward properly.

Network administrators can configure relay entries globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). Multiple relay entries may be configured for the same interface and UDP port, in which case the relay agent unicasts matching packets to each server address. Interface configuration takes priority over global configuration. If the destination UDP port for a packet matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

Network administrators can configure discard relay entries. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

Additionally, administrators can configure which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI, but network administrators can configure a relay entry with any UDP port number. Administrators may configure relay entries that do not specify a destination UDP port. The relay agent assumes that these entries match packets with the UDP destination ports listed in Table 7-1.
Table 7-1. UDP Destination Ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>UDP Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEN-116 Name Service</td>
<td>42</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>NetBIOS Name Server</td>
<td>137</td>
</tr>
<tr>
<td>NetBIOS Datagram Server</td>
<td>138</td>
</tr>
<tr>
<td>TACACS Server</td>
<td>49</td>
</tr>
<tr>
<td>Time Service</td>
<td>37</td>
</tr>
<tr>
<td>DHCP</td>
<td>67</td>
</tr>
<tr>
<td>Trivial File Transfer Protocol</td>
<td>69</td>
</tr>
<tr>
<td>ISAKAMP</td>
<td>500</td>
</tr>
<tr>
<td>Mobile IP</td>
<td>434</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
</tr>
<tr>
<td>PIM Auto RP</td>
<td>496</td>
</tr>
<tr>
<td>RIP</td>
<td>520</td>
</tr>
</tbody>
</table>

Certain pre-existing DHCP relay options do not apply to relay of other protocols. The administrator may optionally set a DHCP maximum hop count or minimum wait time.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers (as a unicast packet), and relays packets to the client that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent verifies that the interface is configured to relay to the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent verifies that there is a global
configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF).
- The destination IP address must be the IPv4 broadcast address (255.255.255.255) or a directed broadcast address for the receiving interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry or an entry in Table 7-1.

DHCP relay cannot be independently enabled or disabled globally. Only IP helper can be enabled or disabled globally. Enabling IP helper enables DHCP relay.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootpdhcprelay maxhopcount</td>
<td>ip helper-address (global configuration)</td>
</tr>
<tr>
<td>bootpdhcprelay minwaittime</td>
<td>ip helper-address (interface configuration)</td>
</tr>
<tr>
<td>clear ip helper statistics</td>
<td>ip helper enable</td>
</tr>
<tr>
<td>ip dhcp relay information check</td>
<td>show ip helper-address</td>
</tr>
<tr>
<td>ip dhcp relay information check-reply</td>
<td>show ip dhcp relay</td>
</tr>
<tr>
<td>ip dhcp relay information option</td>
<td>show ip helper statistics</td>
</tr>
<tr>
<td>ip dhcp relay information option-insert</td>
<td>–</td>
</tr>
</tbody>
</table>
**bootpdhcprelay maxhopcount**

Use the `bootpdhcprelay maxhopcount` command in Global Configuration mode to configure the maximum allowable relay agent hops for BootP/DHCP Relay on the system. Use the no form of the command to set the maximum hop count to the default value.

**Syntax**

```
bootpdhcprelay maxhopcount integer
no bootpdhcprelay maxhopcount
```

- `integer` — Maximum allowable relay agent hops for BootP/DHCP Relay on the system. (Range: 1-16)

**Default Configuration**

The default integer configuration is 4.

**Command Mode**

Global Configuration mode, Virtual Router Configuration mode.

**User Guidelines**

Enable DHCP Relay using the `ip helper enable` command.

When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**

The following example defines a maximum hopcount of 6.

```
console(config)#bootpdhcprelay maxhopcount 6
```
**bootpdhcprelay minwaittime**

Use the **bootpdhcprelay minwaittime** command in Global Configuration mode to configure the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it might use the seconds-since-client- began-booting field of the request as a factor in deciding whether to relay the request or not. Use the no form of the command to set the minimum wait time to the default value.

**Syntax**

bootpdhcprelay minwaittime integer  
no bootpdhcprelay minwaittime

- integer — Minimum wait time for BootP/DHCP Relay on the system.  
  (Range: 0-100 seconds)

**Default Configuration**

0 is the default integer configuration.

**Command Mode**

Global Configuration mode, Virtual Router Configuration mode

**User Guidelines**

Enable DHCP Relay using the **ip helper enable** command.

When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**

The following example defines a minimum wait time of 10 seconds.

```console
console(config)#bootpdhcprelay minwaittime 10
```
clear ip helper statistics

Use the clear ip helper statistics command to reset to 0 the statistics displayed in show ip helper statistics.

Syntax

clear ip helper statistics [vrf vrf-name]
  - vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, counters for the default (global) router instance is cleared.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode

User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.

Example

clear ip helper statistics

dhcp relay information check

Use the dhcp relay information check command to enable DHCP Relay to check that the relay agent information option in forwarded BOOTREPLY messages is valid. If an invalid message is received, the relay agent drops it. This information check will take effect, though enabled, only when the relay agent interface is enabled to insert the suboptions.

Syntax

ip dhcp relay information check
no ip dhcp relay information check
**Default Configuration**
This is enabled by default for a DHCP relay agent.

**Command Mode**
Global Configuration mode, Virtual Router Configuration mode

**User Guidelines**
Enable DHCP Relay using the `ip helper enable` command. Interface configuration takes precedence over global configuration. However if there is no interface configuration then global configuration is followed.

This check is enabled by default. The administrator has to ensure that the relay should be configured such that only it should insert option-82 fields and no other device near the client has the facility to insert options.

When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**
The following example enables relay information check globally:

```
console(config)#ip dhcp relay information check
```

**ip dhcp relay information check-reply**
Use the `ip dhcp relay information check-reply` command to enable DHCP Relay to check that the relay agent information option in forwarded BOOTREPLY messages is valid. If an invalid message is received, the relay agent drops it. This information check will take effect, though enabled, only when the relay agent interface is enabled to insert the suboptions.

**Syntax**

```
ip dhcp relay information check-reply [none]
no ip dhcp relay information check-reply
```

-  **none**—(Optional) Disables the command function.
**Default Configuration**
This check is enabled by default.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
Enable DHCP Relay using the `ip helper enable` command. Use the global configuration command `ip dhcp relay information option` command to enable processing of DHCP circuit ID and remote agent ID options. DHCP replies are checked by default. The network administrator should ensure that only one switch in the path between the DHCP client and server processes DHCP information options.

**Example**
The following example enables relay information check on the interface:
```console
console(config)#interface vlan 10
console(config-if-vlan10)#ip dhcp relay information check-reply
```

**ip dhcp relay information option**
Use the `ip dhcp relay information option` command in Global Configuration mode to globally enable insertion of the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system (also called option 82). Use the `no` form of the command to globally disable the circuit ID option and remote agent ID mode for BootP/DHCP Relay.

**Syntax**
```
ip dhcp relay information option  
no ip dhcp relay information option
```

**Default Configuration**
Disabled is the default configuration.

**Command Mode**
Global Configuration mode, Virtual Router Configuration mode
**User Guidelines**

This command globally enables inclusion of DHCP option 82 in DHCP requests forwarded to the DHCP server. This information may also be relayed on a per interface basis using the `ip dhcp relay information option-insert` command.

Enable DHCP Relay using the `ip helper enable` command.

When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**
The following example enables the circuit ID and remote agent ID options.

```
console(config)#ip dhcp relay information option
```

**ip dhcp relay information option-insert**

Use the `ip dhcp relay information option-insert` command in Interface Configuration mode to enable the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the interface (also called option 82). Use the `no` form of the command to return the configuration to the default.

**Syntax**

```
ip dhcp relay information option-insert [none]
no ip dhcp relay information option-insert
```

- `none`—Use to disable insertion of circuit id and remote agent id options into DHCP requests forwarded to the DHCP server.

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Interface (VLAN) Configuration mode
User Guidelines

Enable DHCP Relay using the `ip helper enable` command. The interface configuration always takes precedence over global configuration. However, if there is no interface configuration, then global configuration is followed. Use the `ip dhcp relay information option` command to globally enable inclusion of Option 82 information in DHCP requests forwarded to a DHCP server.

Example

The following example enables the circuit ID and remote agent ID options on VLAN 10.

```
console(config)#interface vlan 10
console(config-if-vlan10)#ip dhcp relay information option-insert
```

ip helper-address (global configuration)

Use the `ip helper-address (global configuration)` command to configure the relay of certain UDP broadcast packets received on any interface. To delete an IP helper entry, use the no form of this command.

Syntax

```
ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
no ip helper-address [server-address] [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
```

- server-address — The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
- dest-udp-port — A destination UDP port number from 1 to 65535. This parameter need not be configured for DHCP. It must be configured for all other protocols which are to be relayed.
- port-name — The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: `dhcp` (port 67), `domain` (port 53), `isakmp` (port 500), `mobile-ip` (port 434), `nameserver` (port 42),
netbios-dgm (port 138), netbios-ns (port 137), ntp (port 123), pim-auto-rp (port 496), rip (port 520), tacacs (port 49), tftp (port 69), and time (port 37). Other ports must be specified by number.

Default Configuration
No helper addresses are configured.

Command Mode
Global Configuration mode, Virtual Router Configuration mode

User Guidelines
This command can be invoked multiple times, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server. Broadcast packets other than DHCP require configuration of a destination UDP port number for IP helper if they are not already listed in Table 7-1. The switch is able to supply the appropriate UDP destination port numbers by examining the DHCP message, so configuration of a UDP destination port is not required for unicast forwarding of DHCP.

The command no ip helper-address with no arguments clears all global IP helper addresses.

When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

Example
To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
console#config
console(config)#ip helper-address 10.1.1.1 dhcp
console(config)#ip helper-address 10.1.2.1 dhcp
```

To relay UDP packets received on any interface for all default ports (see Table 7-1) to the server at 20.1.1.1, use the following commands:

```
console#config
console(config)#ip helper-address 20.1.1.1
```
Command History
Description revised in 6.3.5 release.

ip helper-address (interface configuration)
Use the ip helper-address (interface configuration) command to configure the relay of certain UDP broadcast packets received on a specific interface. To delete a relay entry on an interface, use the no form of this command.

Syntax
ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
no ip helper-address [server-address | discard] [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

• server-address — The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
• discard — Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
• dest-udp-port — A destination UDP port number from 1 to 65535.
• port-name — The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: dhcp (port 67), domain (port 53), isakmp (port 500), mobile-ip (port 434), nameserver (port 42), netbios-dgm (port 138), netbios-ns (port 137), ntp (port 123), pim-auto-rp (port 496), rip (port 520), tacacs (port 49), tftp (port 69), and time (port 37). Other ports must be specified by number.

Default Configuration
No helper addresses are configured.

Command Mode
Interface Configuration (VLAN) mode.
User Guidelines

This command can be invoked multiple times on routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server. Broadcast packets other than DHCP require configuration of a destination UDP port number for IP helper if not listed in Table 7-1. The switch is able to supply the appropriate UDP destination port numbers by examining the DHCP message, so configuration of a UDP destination port is not required for unicast forwarding of DHCP.

The command no ip helper-address with no arguments clears all helper addresses on the interface.

Example

To relay DHCP packets received on vlan 5 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```console
console#config
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address 192.168.10.1 dhcp
console(config-if-vlan5)#ip helper-address 192.168.20.1 dhcp
```

To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```console
console#config
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address 192.168.30.1 dhcp
console(config-if-vlan5)#ip helper-address 192.168.30.1 domain
```

This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than VLAN 5 and VLAN 6 to 192.168.40.1, relays DHCP and DNS packets received on VLAN 5 to 192.168.40.2, relays SNMP traps (port 162) received on interface VLAN 6 to 192.168.23.1, and drops DHCP packets received on VLAN 6:

```console
console#config
console(config)#ip helper-address 192.168.40.1 dhcp
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address 192.168.40.2 dhcp
console(config-if-vlan5)#ip helper-address 192.168.40.2 domain
console(config-if-vlan5)#exit
console(config)#interface vlan 6
console(config-if-vlan6)#ip helper-address 192.168.23.1 162
console(config-if-vlan6)#ip helper-address discard dhcp
```
Command History
Description revised in 6.3.5 release.

ip helper enable
Use the ip helper enable command to enable relay of UDP packets. To disable relay of all UDP packets, use the “no” form of this command.

Syntax
ip helper enable
no ip helper enable

Default Configuration
IP helper is enabled by default.

Command Mode
Global Configuration mode

User Guidelines
This command can be used to temporarily disable IP helper without deleting all IP helper addresses.
This command replaces the bootpdhcprelay enable command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.
When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.
Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

Example
console(config)#ip helper enable
**show ip helper-address**

Use the `show ip helper-address` command to display the IP helper address configuration.

**Syntax**

`show ip helper-address [vrf vrf-name] [interface]`

- `interface` — Optionally specify an interface to limit the output to the configuration of a single interface. The interface is identified as vlan vlan-id.
- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The following output is shown:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The relay configuration is applied to packets that arrive on this interface. This field is set to “any” for global IP helper entries.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as “any” are applied to packets with the destination UDP ports listed in Table 7-1.</td>
</tr>
</tbody>
</table>
### Layer 3 Routing Commands

#### Example

```
show ip helper-address

IP helper is enabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>UDP Port</th>
<th>Discard</th>
<th>Hit Count</th>
<th>Server Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 100</td>
<td>dhcp</td>
<td>No</td>
<td>10</td>
<td>10.100.1.254</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.100.2.254</td>
</tr>
<tr>
<td>vlan 101</td>
<td>any</td>
<td>Yes</td>
<td>2</td>
<td>10.200.1.254</td>
</tr>
<tr>
<td>any</td>
<td>dhcp</td>
<td>No</td>
<td>0</td>
<td>10.200.1.254</td>
</tr>
</tbody>
</table>
```

### show ip dhcp relay

Use the `show ip dhcp relay` command in User Exec mode to display the BootP/DHCP Relay information.

#### Syntax

```
show ip dhcp relay [vrf vrf-name] [interface vlan vlan-id]
```

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- **vlan-id**—A valid VLAN identifier.

#### Default Configuration

The command has no default configuration.

#### Command Mode

User Exec and Privileged Exec modes, Global Configuration mode and all Configuration submodes
**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example**

The following example defines the Boot/DHCP Relay information.

```
console#show ip dhcp relay
```

- Maximum Hop Count.............................. 4
- Minimum Wait Time (Seconds).................... 0
- Circuit Id Option Mode....................... Disable
- Circuit Id Option Check Mode.................. Enable

**show ip helper statistics**

Use the `show ip helper statistics` command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

**Syntax**

```
show ip helper statistics [vrf vrf-name]
```

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.
The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP client messages received</td>
<td>The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL &gt; 1 and having valid source and destination IP addresses.</td>
</tr>
<tr>
<td>DHCP client messages relayed</td>
<td>The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.</td>
</tr>
<tr>
<td>DHCP server messages received</td>
<td>The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.</td>
</tr>
<tr>
<td>DHCP server messages relayed</td>
<td>The number of DHCP server messages relayed to a client.</td>
</tr>
<tr>
<td>UDP client messages received</td>
<td>The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.</td>
</tr>
<tr>
<td>UDP client messages relayed</td>
<td>The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.</td>
</tr>
<tr>
<td>DHCP message hop count exceeded max</td>
<td>The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show ip dhcp relay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.</td>
</tr>
<tr>
<td>DHCP message with secs field below min</td>
<td>The number of DHCP client messages received with secs fields that are less than the minimum value. The minimum secs value is a configurable value and is displayed in show ip dhcp relay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.</td>
</tr>
</tbody>
</table>
**Example**

```console
console#show ip helper statistics

DHCP client messages received.................. 8
DHCP client messages relayed................... 2
DHCP server messages received................... 2
DHCP server messages relayed................... 2
UDP client messages received................... 8
UDP client messages relayed.................... 2
DHCP message hop count exceeded max............ 0
DHCP message with secs field below min......... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL....................... 0
Packets that matched a discard entry........... 0
```
IP Routing Commands

Dell EMC Networking N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Dell Network N1500/N2000/N2100-ON series supports limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

Dell EMC Networking routing provides the base Layer 3 support for Local Area Network (LAN) and Wide Area Network (WAN) environments. The Dell EMC Networking switches allows the network operator to build a complete Layer 3+ configuration with advanced functionality. As the Dell EMC Networking defaults to Layer 2 switching functionality, routing must be explicitly enabled on the Dell EMC Networking to perform Layer 3 forwarding. For Dell EMC Networking switches, routing is only supported on VLAN and Loopback interfaces for in-band ports. It is not possible to route packets to or from the out-of-band interface.

Static Routes/ECMP Static Routes

The operator is able to configure static and default routes with multiple next hops to any given destination. Permitting the additional routes creates several options for the Dell EMC Networking switch operator.

1. The operator configures multiple next hops to a given destination, intending for the router to load share across the next hops.

2. The operator configures multiple next hops to a given destination, intending for the router to use the primary next hops and only use the other next hops if the primary next hops are unusable.

The operator distinguishes static routes by specifying a route preference value. A static route with a lower preference value is a more preferred static route. Next hops with the same preference are grouped into a single ECMP route. A less preferred static route is used if the more preferred static route is unusable. (The link is down or the next hop IP address cannot be resolved to a MAC address.)

In Dell EMC Networking, the operator deletes an individual next hop from a static route or deletes an entire static route at once. The cost of a static route is always 1 unless configured otherwise by the operator.
The addition of a preference option has a side benefit. The preference option allows the operator to control the preference of individual static routes relative to routes learned from other sources (such as OSPF). When routes from different sources have the same preference, Dell EMC Networking routing prefers a static route over a dynamic route.

### Static Reject Routes

To administratively control the traffic destined to a particular network so that it is not forwarded through the router, Dell EMC Networking enables configuring a static reject route for that network on the router. Such traffic is discarded and an ICMP destination unreachable message is sent back to the source. Static reject routes are typically used to prevent routing loops.

### Default Routes

Dell EMC Networking routing provides a preference option for the configuration of default routes. A configured default route is treated exactly like a static route. Therefore, default routes and static routes have the same default preference (1).

### Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>ip unnumbered</td>
<td>show ip brief</td>
</tr>
<tr>
<td>ip icmp echo-reply</td>
<td>ip unnumbered gratuitous-arp</td>
<td>Maximum Next Hops................</td>
</tr>
<tr>
<td>ip netdirbcast</td>
<td>match ip address</td>
<td>show ip policy</td>
</tr>
<tr>
<td>ip policy route-map</td>
<td>match length</td>
<td>show ip protocols</td>
</tr>
<tr>
<td>ip redirects</td>
<td>match mac-list</td>
<td>show ip route</td>
</tr>
<tr>
<td>ip route</td>
<td>route-map</td>
<td>show ip route static</td>
</tr>
<tr>
<td>ip route default</td>
<td>set interface null0</td>
<td>show ip route preferences</td>
</tr>
<tr>
<td></td>
<td>set ip default next-hop</td>
<td>show ip route summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show ip traffic</td>
</tr>
</tbody>
</table>

Layer 3 Routing Commands | 1504
**encapsulation**

Use the `encapsulation` command in Interface Configuration (VLAN) mode to configure the Link Layer encapsulation type for the packet. Routed frames are always Ethernet-encapsulated when a frame is routed to a VLAN.

**Syntax**

```
encapsulation {ethernet | snap}
```

- **ethernet** — Specifies Ethernet encapsulation.
- **snap** — Specifies SNAP encapsulation.

**Default Configuration**

Ethernet encapsulation is the default configuration.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example applies SNAP encapsulation for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#encapsulation snap
```

**ip icmp echo-reply**

Use the `ip icmp echo-reply` command to enable or disable the generation of ICMP Echo Reply messages. Use the `no` form of this command to prevent the generation of ICMP Echo Replies.
Syntax
ip icmp echo-reply
no ip icmp echo-reply

Default Configuration
ICMP Echo Reply messages are enabled by default.

Command Mode
Global Configuration mode, Virtual Router Configuration mode

User Guidelines
When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

Example
console(config)#ip icmp echo-reply

ip icmp error-interval
Use the ip icmp error-interval command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket with two configurable parameters: Burst-size and burst-interval. To disable ICMP rate limiting, set burst-interval to zero. Use the no form of this command to return burst-interval and burst-size to their default values.

Syntax
ip icmp error-interval burst-interval [ burst-size ]
no ip icmp error-interval
• burst-interval — How often the token bucket is initialized (Range: 0–2147483647 milliseconds).
• burst-size — The maximum number of messages that can be sent during a burst interval (Range: 1–200).
**Default Configuration**
Rate limiting is enabled by default.
The default burst-interval is 1000 milliseconds.
The default burst-size is 100 messages.

**Command Mode**
Global Configuration mode, Virtual Router Configuration mode

**User Guidelines**
There are no user guidelines for this command.
When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**
```
console(config)#ip icmp error-interval 1000 20
```

**ip netdirbcast**
Use the `ip netdirbcast` command in Interface Configuration mode to enable the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped. Use the no form of the command to disable the broadcasts.

**Syntax**
- `ip netdirbcast`
- `no ip netdirbcast`

**Default Configuration**
Disabled is the default configuration.

**Command Mode**
Interface Configuration (VLAN) mode
User Guidelines
This command has no user guidelines.

Example
The following example defines the IP address and subnet mask for VLAN 15.

console(config)#interface vlan 15
console(config-if-vlan15)#ip netdirbcast

ip policy route-map
Use this command to apply a route map on an interface. Use the no form of this command to delete a route map from the interface.

Syntax
ip policy route-map map-tag
no ip policy route-map map-tag
  • map-tag—Name of the route map to use for policy based routing. It must match a map tag specified by the route-map command.

Default Configuration
No route maps are configured by default.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Policy-based routing must be configured on the VLAN interface that receives the packets, not on the VLAN interface from which the packets are sent. Packets matching a deny route map are routed using the routing table. Policy maps with no set clause are ignored.

When a route-map applied on an interface is changed, i.e. new statements are added to route-map or match or set terms are added/removed from the route-map statement, or if any route-map that is applied on an interface is removed,
the entire sequence of route-maps needs to be removed from the interface and added back again in order to have the changed route-map configuration be effective.

If the administrator removes match or set terms in a route-map intermittently, the counters corresponding to the removed match term are reset to zero.

A route-map statement must contain eligible match/set conditions for policy based routing in order to be applied to hardware.

Valid match conditions are:
match ip address <acl>, match mac-list, match length

Valid set conditions are:
set ip next-hop, set ip default next-hop, set ip precedence

A route-map statement must contain at least one of the match and one of the set conditions specified above in order to be eligible to be applied to hardware. If not, the route-map is not applied to hardware.

An ACL referenced in a route-map may not be edited. Instead, create a new ACL with the desired changes and update the route-map with the edited ACL.

Route-maps and DiffServ cannot operate on the same interface due to allocation of conflicting resources. An error is thrown to user if when configuring a route-map on an interface on which DiffServ has been previously configured.

When a route map is configured on a VLAN interface and a DiffServ policy is applied on any individual member port of the same VLAN interface, the port policy (DiffServ) takes priority over the VLAN (route map) policy.

**Example**

Considering equal-access as a route-map configured earlier, the following sequence is an example of how a route map is applied to a VLAN.

```
console(config)#interface vlan 10
console(config-if-vlan10)#ip policy route-map equal-access
```
ip redirects

Use the `ip redirects` command to enable the generation of ICMP Redirect messages. Use the `no` form of this command to prevent the sending of ICMP Redirect Messages. In global configuration mode, this command affects all interfaces. In interface configuration mode, it only affects that interface.

**Syntax**

```
ip redirects
no ip redirects
```

**Default Configuration**

ICMP Redirect messages are enabled by default.

**Command Mode**

Global Configuration mode, Virtual Router Configuration mode, Interface Configuration (VLAN) mode

**User Guidelines**

When in virtual router configuration mode, this command operates within the context of the virtual router instance. When in global config mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**

```
console(config-if-vlan10)#ip redirects
```

ip route

Use the `ip route` command in Global Configuration mode to configure a static route. Use the `no` form of the command to delete the static route.

**Syntax**

```
ip route [vrf vrf-name] networkaddr {subnetmask | prefix-length} {Null 0 | nexthopip | vlan vlan-id [nexthopip]} [preference] [name text]
```
no ip route [vrf vrf-name] networkaddr {subnetmask | prefix-length} {Null 0
| nexthopip | vlan vlan-id [nexthopip]}

- vrf-name—The name of the VRF if which the route is to be installed. If no
  vrf is specified, the route is created in the global routing table.
- networkaddr — IP address of destination interface.
- subnetmask—A 32 bit dotted-quad subnet mask. Enabled bits in the mask
  indicate the corresponding bits of the network address are significant.
  Enabled bits in the mask must be contiguous.
- prefix-length—A forward slash followed by an integer number ranging
  from 1-32 (e.g., /24). The integer number indicates the number of
  significant bits in the address beginning with the leftmost (most
  significant) bit.
- nexthopip—The next-hop IPv4 address is specified in the argument
  nexthopip. Packets matching the destination route are forwarded to the
  next hop IP address.
- vlan-id—A configured VLAN routing interface identifier for a VRF or an
  IP unnumbered interface. If a VLAN routing interface for a VRF is
  specified, it imports the associated subnet into the default routing
  instance from the VRF associated with the VLAN.
- Null0—The optional Null0 keyword indicates that packets matching the
  route are dropped. This capability allows the administrator to purposefully
  implement a black hole for selected traffic.
- text—A textual name for the route as configured by the administrator.
  May be up to 32 characters in length.

**Default Configuration**

Default value of preference is 1. The router will prefer a route with a smaller
administrative distance that a route with a higher administrative distance.

**Command Mode**

Global Configuration mode
**User Guidelines**

The IP route command sets a value for the route preference. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. Specifying the preference of a static route controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

The ip route command optionally configures a route in the selected VRF. The IP route command can set a value for the route preference. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database.

Specifying the preference of a static route controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

This command creates a static route in a specified virtual router instance referred to by name ‘vrf-name’ by taking an optional vrf argument. If the next-hop interface argument is given without specifying a nexthopip, it is added as a static interface route. If the next-hop interface is in the default routing domain, they routes are identified as leaked routes in the virtual router table.

The VRF identified in the parameter must have been previously created or an error is returned.

Route leaking in VRFs is only supported to or from the default routing instance and only for static routes. Configuring a leaked route from a non-default VRF to another non-default VRF results in undefined behavior.

Only IPv4 routes are supported with the vrf parameter.

Adding a static route with a Null 0 next hop specified configures a routing black hole (a static reject route). Packets destined to that prefix are dropped.

If an interface for the next hop is specified, it may be a numbered or unnumbered interface.

A static route entry is only installed if the next hop IP address matches one of the local subnets (i.e., the next hop is reachable). In case of unnumbered interfaces, static routes entries created for an unnumbered-peer do not match with any of the local subnets. By specifying the interface explicitly in the
static route command along with the next hop IP address, the switch can correctly install static route entries for unnumbered-peers. It is also possible to configure ‘unnumbered interface routes’ where the next hop IP address is not specified and only the unnumbered nexthop interface is configured.

**Examples**

**Route Leaking Example 1**

The following shows the configuration for VRF red-1 configured in VLAN 10. A static global route for the 172.16.0.0 with a next hop of 172.16.0.2 is injected into VRF red-1.

```
configure
vlan 10
exit
ip vrf red-1
ip routing
exit
ip routing
ip route vrf red-1 172.16.0.0 255.240.0.0 172.16.0.2
interface vlan 1
ip address 172.16.0.1 255.240.0.0
exit
interface vlan 10
ip vrf forwarding red-1
ip address 192.168.0.1 255.255.255.0
ip ospf area 0
exit
router ospf vrf "red-1"
router-id 1.1.1.1
network 192.168.0.0 0.0.0.255 area 0
exit
!
interface Gi1/0/1
switchport mode trunk
switchport access vlan 10
exit
!
interface loopback 0
ip vrf forwarding red-1
ip address 1.1.1.1 255.255.255.255
exit
```
Route Leaking Example 2

Subnetwork 9.0.0.0/24 is a directly connected subnetwork on VLAN 10 in the default routing table.

Subnet 8.0.0.0/24 is a directly connected subnetwork in VLAN 30 in virtual router Red.

Subnet 66.6.6.x is reachable via VLAN 30 in vrf Red.

The first `ip route` command below leaks the 66.6.6.x subnet from vrf Red into the default routing table.

The second `ip route` command configures a gateway for the default routing table.

The next `ip route` commands leak the 9.0.0.x route from the default route table into the virtual router Red.

The last `ip route` command configures the 66.6.6.x subnet as reachable via next hop 8.0.0.2 in Vrf Red.

```console
configure
vlan 10,30
exit
ip vrf Red
ip routing
exit
ip routing
interface vlan 10
ip address 9.0.0.1 255.255.255.0
exit
interface vlan 30
ip vrf forwarding Red
ip address 8.0.0.1 255.255.255.0
exit
ip route 66.6.6.0 255.255.255.0 Vl30
ip route 0.0.0.0 0.0.0.0 9.0.0.2 253
ip route vrf Red 9.0.0.0 255.255.255.0 Vl10
ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
!
interface Gi1/0/1
switchport access vlan 10
exit
!
interface Gi1/0/3
switchport access vlan 30
exit

console(config)#show ip route
```
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, E - Externally Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
S U - Unnumbered Peer, L - Leaked Route

* Indicates the best (lowest metric) route for the subnet.

Default Gateway is 9.0.0.2
S  *0.0.0.0/0 [253/0] via 9.0.0.2,  Vl10
C  *9.0.0.0/24 [0/1] directly connected,  Vl10
L  *66.6.6.0/24 [1/0] via 0.0.0.0,  Vl10

console(config)#show ip route vrf Red

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, E - Externally Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
S U - Unnumbered Peer, L - Leaked Route

* Indicates the best (lowest metric) route for the subnet.

No default gateway is configured.
C  *8.0.0.0/24 [0/1] directly connected,  Vl130
L  *9.0.0.0/24 [1/0] via 0.0.0.0,  Vl10
S  *66.6.6.0/24 [1/0] via 8.0.0.2,  Vl130

ip route default

Use the ip route default command in Global Configuration mode to
configure the next hop address of the default route. Use the no form of the
command to delete the default route.

Use of the optional VRF parameter executes the command within the
context of the VRF specific routing table.

Syntax

ip route default [vrf vrf-name] next-hop-ip [preference]
no ip route default next-hop-ip [preference]

•  vrf-name—The name of the VRF associated with the routing table context
  used by the command. If no vrf is specified, the global routing table
  context is used.
•  next-hop-ip — IP address of the next hop router.
- **preference** — Specifies the preference value, a.k.a administrative distance, of an individual static route. (Range: 1-255)

**Default Configuration**
Default value of preference is 1.

**Command Mode**
Global Configuration mode

**User Guidelines**
For routed management traffic:
1. Router entries are checked for applicable destinations.
2. The globally assigned default-gateway is consulted.

If DHCP is enabled on multiple in-band interfaces and the system learns a different default gateway on each, the system retains the first default gateway it learns and ignores any others. If the first default gateway is lost, the system does not revert to an alternate default gateway until it renews its IP address.

Using this command, the administrator may manually configure a single, global default gateway. The switch installs a default route for a configured default gateway with a preference of 253, making it more preferred than the default gateways learned via DHCP, but less preferred than a static default route. The preference of these routes is not configurable.

The switch installs a default route for the default gateway whether or not routing is globally enabled. When the user displays the routing table (e.g. `show ip route`), the display identifies the default gateway, if one is known.

Use the `show ip route static all` command to display the configured static routes and preferences.

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the `vrf` parameter.
This command is only available on the N3000/N3100/N4000 switches.
Example
The following example identifies the next-hop-ip and a preference value of 200.

console(config)#ip route default 192.168.10.1 200

ip route distance

Use the ip route distance command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The ip route and ip route default commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance are applied to static routes created after invoking the ip route distance command.

Use of the optional vrf parameter executes the command within the context of the VRF specific routing table.

Syntax

ip route distance [vrf vrf-name]integer
no ip route distance integer

• vrf-name—The name of the VRF associated with the routing table context used by the command. If no vrf is specified, the global routing table context is used.

• integer — Specifies the distance (preference) of an individual static route. (Range 1-255)

Default Configuration
Default value of distance is 1.

Command Mode
Global Configuration mode
User Guidelines
Lower route distance values are preferred when determining the best route. The VRF identified in the parameter must have been previously created or an error is returned.
Only IPv4 addresses are supported with the vrf parameter.
This command is only available on the N3000/N3100/N4000 switches.

Example
The following example sets the default route metric to 80.

```
console(config)#ip route distance 80
```

ip routing
Use the ip routing command in Global Configuration mode to globally enable IPv4 routing on the router. To disable IPv4 routing globally, use the no form of the command.

Syntax
ip routing
no ip routing

Default Configuration
Disabled is the default configuration.

Command Mode
Global Configuration mode, Virtual Router Configuration mode

User Guidelines
Use the show ip brief command to determine if routing is enabled or disabled. When in virtual router configuration mode, this command operates within the context of the virtual router instance. When in global config mode, the command operates on the global router instance.
Enable IPv4 routing on a VLAN by entering `interface vlan mode` for the desired VLAN and assigning an IP address to the VLAN. Use the `no interface vlan` command to disable routing on an interface. Ensure that statically assigned addresses do not conflict with any configured subnets. Subnet overlap is not allowed.

Virtual Router Configuration mode is only available on the N3000/N3100/N4000 switches.

**Example**
The following example enables IPv4 routing for VLAN 15

```
console(config)#vlan 15
console(config-vlan15)#interface vlan 15
console(config-if-vlan15)#ip address 10.0.3.2 /8
console(config-if-vlan15)#exit
console(config)#ip routing
```

**ip unnumbered**
This command is used to identify an interface as an unnumbered interface and specify the numbered interface providing the borrowed address. The numbered interface must be a loopback interface. To stop borrowing an address, use the `no` form of the command.

**Syntax**
ip unnumbered loopback loopback-id
no ip unnumbered
- loopback-id—The loopback identifier (Range 0–7)

**Default Configuration**
The are no ip unnumbered interfaces by default.

**Command Mode**
Interface (VLAN) Configuration

**User Guidelines**
IP unnumbered interfaces are supported in the default VRF only.
The interface should be configured as able to borrow an IP address, i.e. a routing interface with no IP address.

The loopback interface is the numbered interface providing the borrowed address. The providing loopback interface cannot be unnumbered. The loopback interface is identified by its loopback interface number.

It is a misconfiguration for two routers, R1 and R2, to be connected by a link where R1’s interface is unnumbered and R2’s interface is numbered. If a static route is configured on R2 using R1’s IP address as next hop, the static route will never be installed in the routing table because the next hop is not in a local subnet. If a static route is configured on R1 using R2’s IP address as next hop, the static route will be installed in the routing table. R1 will ARP for the next hop address. R2 will ignore the ARP Request because the source IP address is not in a local subnet.

It is a misconfiguration to enable OSPF on both ends of an unnumbered interface without setting the OSPF network type to point-to-point. Each router will reject its neighbor’s HELLOs because the source IP address is not in a local subnet. Adjacencies never progress beyond the INIT state.

If three or more routers are connected to the same subnet/broadcast domain and all are configured to treat the Ethernet interface as a point-to-point link, adjacencies may not form. The OSPF database description packets intended for a specific neighbor will be processed by all neighbors, causing errors that reset adjacencies.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-if-vlan1)#ip unnumbered 10.130.14.55
```

**ip unnumbered gratuitous-arp accept**

This command enables installation of a static interface route to the unnumbered peer upon receiving a gratuitous ARP.

**Syntax**

```
ip unnumbered gratuitous-arp accept
```
no ip unnumbered gratuitous-arp accept

**Default Configuration**
The default mode is accept.

**Command Mode**
Interface (VLAN) Configuration

**User Guidelines**
IP unnumbered interfaces are supported in the default VRF only.
The interface should be configured as able to borrow an IP address, i.e. a routing interface with no IP address.
Normally, the static ARP entry is only installed if the IP address matches one of the local subnets. In case of unnumbered interfaces, static ARP entries created for the unnumbered-peer do not match any of the local subnets. By specifying the interface explicitly in the static ARP command, static ARP entries for unnumbered-peers can be installed in the ARP table.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config-if-vlan1)#ip unnumbered gratuitous-arp accept
```

**ip unreachables**
Use the *ip unreachables* command to enable the generation of ICMP Destination Unreachable messages. Use the *no* form of this command to prevent the generation of ICMP Destination Unreachable messages.

**Syntax**

```
ip unreachables
no ip unreachables
```
**Default Configuration**
ICMP Destination Unreachable messages are enabled.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-if-vlan10)#ip unreachable
```

**match ip address**
Use this command to specify IP address match criteria for a route map. Use the no form of this command to delete a match statement from a route map.

**Syntax**
```
match ip address access-list-name [access-list-name]
no match ip address [access-list-name]
```

- access-list-name—The access-list name that identifies the named IP ACLs. The name can be up to 31 characters in length.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Route Map Configuration mode

**User Guidelines**
The IP ACL must be configured before it can be linked to a route-map. Specifying an unconfigured IP ACL causes an error. Actions present in an IP ACL configuration are applied along with other actions present in route-map. When IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.
Actions in the IP ACL configuration are applied with other actions present in the route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from the ACL, the configuration is rejected.

If a list of IP access lists is specified in this command and a packet matches at least one of these access list match criteria, the corresponding set of actions in the route map are applied to the packet. Duplicate IP access list names are ignored.

It is strongly recommended that access lists used in a route map not be re-used for normal access list processing. This is because:

- ACLs inherit the priority of the route map. This overrides the priority of the including access group.
- Route maps do not have a implicit deny all at the end of the list. Instead, non-matching packets for a permit route map use the routing table.

### Example

The example below creates two access lists (R1 and R2) and two route-maps with IP address match clauses and that associate the route-map to an interface.

In the example, the ip policy route-map equal-access command is applied to interface VLAN 11. All packets ingressing VLAN 11 are policy-routed.

Route map sequence 10 in route map equal-access is used to match all packets sourced from any host in subnet 10.1.0.0. If there is a match, and if the router has no explicit route for the packet’s destination, it is sent to next-hop address 192.168.6.6.

Route map sequence 20 in route map equal-access is used to match all packets sourced from any host in subnet 10.2.0.0. If there is a match, and if the router has no explicit route for the packet’s destination, it is sent to next-hop address 172.16.7.7.

All other packets are forwarded as per normal L3 destination-based routing.

```
console(config-if-vlan3)#ip policy route-map equal-access

console(config)#ip access-list R1
console(config-ip-acl)#permit ip 10.1.0.0 0.0.255.255 any
console(config-ip-acl)#exit

console(config)#ip access-list R2
console(config-ip-acl)#permit ip 10.2.0.0 0.0.255.255 any
console(config-ip-acl)#exit
```
```
course(config)#route-map equal-access permit 10
console(config-route-map)#match ip address R1
console(config-route-map)#set ip default next-hop 192.168.6.6
console(config-route-map)#exit

console(config)#route-map equal-access permit 20
console(config-route-map)#match ip address R2
console(config-route-map)#set ip default next-hop 172.16.7.7
console(config-route-map)#exit

console(config)#interface vlan 11
console(config-if-vlan11)#ip address 10.1.1.1 255.255.255.0
console(config-if-vlan11)#ip policy route-map equal-access

console(config)#interface vlan 12
console(config-if-vlan12)#ip address 10.1.1.1 255.255.255.0
console(config-if-vlan12)#ip policy route-map equal-access

console(config)#interface vlan 13
console(config-if-vlan13)#ip address 192.168.6.5 255.255.255.0

console(config)#interface vlan 16
console(config-if-vlan16)#ip address 172.16.7.6 255.255.255.0

This example illustrates the scenario where IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

console#show ip access-lists
Current number of ACLs: 9  Maximum number of ACLs: 100

<table>
<thead>
<tr>
<th>ACL ID/Name</th>
<th>Rules</th>
<th>Interface(s)</th>
<th>Direction</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>madan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

console#show mac access-lists

Current number of all ACLs: 9  Maximum number of all ACLs: 100

<table>
<thead>
<tr>
<th>MAC ACL Name</th>
<th>Rules</th>
<th>Interface(s)</th>
<th>Direction</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>madan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mohan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>goud</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
console(config)#route-map madan
console(route-map)#match ip address 1 2 3 4 5 madan
console(route-map)#match mac-list madan mohan goud
console(route-map)#exit
console(config)#exit
console #show route-map

route-map madan permit 10
   Match clauses:
   ip address (access-lists) : 1 2 3 4 5 madan
   mac-list (access-lists) : madan mohan goud
   Set clauses:

console(config)#access-list 2 permit every
Request denied. Another application using this ACL restricts the number of rules allowed.

custom(config)#ip access-list madan

custom(config-ipv4-acl)#permit udp any any
Request denied. Another application using this ACL restricts the number of rules allowed.

**match length**

Use this command to configure packet length matching criteria for a route map. Use the no form of this command to delete a match statement from a route map.

**Syntax**

**match length** min max

**no match length**

- **min**—Specifies the minimum Layer 3 length for the packet, inclusive, allowing for a match.
- **max**—Specifies the maximum Layer 3 length for the packet, inclusive, allowing for a match.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Route Map mode

**User Guidelines**
The match criteria specified by this command acts on the packet length as it appears in the IP header and is not necessarily correlated with the frame length as it appears on the wire.

**Example**
```
console(config-route-map)#match length 64 1500
```

**match mac-list**
Use this command to configure MAC ACL match criteria for a route map. Use the no form of this command to delete the match statement from a route map.

**Syntax**
```
match mac-list mac-list-name [mac-list-name]
no match mac-list [mac-list-name]
```

- mac-list-name—The MAC ACL name that identifies the MAC ACLs. The name can be between 0 and 31 characters.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Route Map mode

**User Guidelines**
The MAC ACL must be configured before it is linked to a route map. Trying to link to an unconfigured MAC ACL causes an error.
Actions in the MAC ACL configuration are applied with other actions configured in the route map. When a MAC ACL referenced by a route map is removed, the route map rule is also removed.

Example

```
console(config-route-map)#match mac-list mac-test
```

**route-map**

Use this command to create a policy based route map. Use the `no` form of this command to delete a route map or one of its statements.

**Syntax**

```
route-map map-tag [permit | deny] [sequence-number]
```

```
no route-map map-tag [permit | deny] [sequence-number]
```

- **map-tag**—Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long and comprised of any printable character except a question mark. Enclose the map-tag in quotes to embed blanks in the name.

- **permit**—(Optional) Permit routes that match all of the match conditions in the route map.

- **deny**—(Optional) Deny routes that match all of the match conditions in the route map. Packets matching deny routes use the routing table.

- **sequence-number**—(Optional) An integer used to order the set of route maps. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

**Default Configuration**

No route maps are configured by default. If no permit or deny tag is specified, `permit` is the default.

**Command Mode**

Global Configuration mode
**User Guidelines**

Apply an ACL rule on the VLAN interface to perform policy based routing based on the VLAN ID as a matching criteria for incoming packets. Packets matching a deny rule or a deny route-map are routed using the routing table.

There is no implicit deny all at the end of a route map. Packets not matching any clause are routed using the routing table.

Route maps with no set clause are ignored. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed.

Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed.

**Examples**

The following example creates (or edits) the route map equal-access as the first route map in the system for allowing matching packets into the system. Route-map mode is also entered.

```
console(config)# route-map equal-access permit 0
```

In the following example, BGP is configured to redistribute all prefixes within 172.20.0.0 and reject all others.

```
console(config)# ip prefix-list redist-pl permit 172.20.0.0/16 le 32
console(config)# route-map redist-rm permit
console(config-route-map)# match ip address prefix-list redist-pl
console(config-route-map)# exit
console(config)# router bgp 1
console(Config-router) redistribute ospf route-map redist-rm
```
**set interface null0**

Use this command to drop a packet instead of reverting to normal routing for packets that do not match the route map criteria. This command should be configured as the last entry in the route-map as no further set clauses will operate on a dropped packet. Use the no form of this command to remove the set clause from a route map.

**Syntax**

```
set interface null0
no set interface null0
```

- null0—Specifies the null0 interface used to drop packets.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Route Map mode

**User Guidelines**

A route-map statement used for policy based routing is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit and the packet meets all the match criteria, the set clauses in the route-map statement are applied. If no match is found in the route-map, the packet is forwarded using the routing decision resulting from traditional destination-based routing. If the network administrator does not want to revert to normal forwarding but instead want to drop packets that do not match the specified criteria, a set clause routing the packets to interface null0 may be configured as the last (highest numbered) route-map.

**Example**

```
console(config-route-map)#set interface null0
```
set ip default next-hop

Use this route map clause to override default entries in the routing table. Packets that can routed by an active explicit route in the routing table are not affected by this clause. Use this command to set a list of default next-hop IP addresses to be used if no explicit route for the packet’s destination address appears in the routing table. If more than one IP address is specified, the reachable address in the list is used. Use the no form of this command to remove a set command from a route map.

Syntax

set ip default next-hop ip-address [ip-address]
no set ip default next-hop ip-address [ip-address]

ip-address—The IP address of the next hop to which packets are routed. It must be the address of an adjacent router.
• ip-address—A maximum of 16 next-hop IP addresses can be specified.

Default Configuration

There is no default configuration for this command.

Command Mode

Route Map mode

User Guidelines

A packet is routed to the next hop specified by this command only if there is no active explicit route for the packet’s destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

Only one of set ip next-hop, set ip default next-hop, or set interface null0 may be specified in a route map.

Example

custom(config-route-map)#set ip default next-hop 192.0.2.2
**set ip next-hop**

Use this command to specify an adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a link up interface is used to route the packets. Use the no form of this command to remove a set command from a route map.

**Syntax**

`set ip next-hop ip-address [ip-address]`

`no set ip next-hop ip-address [ip-address]`

- ip-address—The IP address of the next hop to which packets are routed. It must be the address of an adjacent router (i.e., the next hop must be in a subnet configured on the local router). A maximum of 16 next-hop IP addresses can be specified.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Route Map mode

**User Guidelines**

Use this route map clause to override active routes in the routing table. This command affects all matching packet types and is used if an active route for the next hop exists in the routing table. The next hop IP address must be associated with a directly connected subnet on the router. If no resolvable active interface is present in the route table, the packet is routed using the default routing table.

Only one of set ip next-hop, set ip default next-hop, or set interface null0 may be specified in a route map.

**Example**

```
console(config-route-map)#set ip next-hop 192.0.2.1
```
set ip precedence

Use this command to set the three IP precedence bits in the IP packet header on ingress. Values 0 through 7 are supported. This precedence value may be used by other QoS services in the switch such as weighted fair queuing (WFQ) or weighted random early detection (WRED). Use the no form of this command to remove a set clause from a route map.

Syntax

set ip precedence 0-7
no set ip precedence

• 0—Sets the routine precedence.
• 1—Sets the priority precedence.
• 2—Sets the immediate precedence.
• 3—Sets the Flash precedence.
• 4—Sets the Flash override precedence.
• 5—Sets the critical precedence.
• 6—Sets the internetwork control precedence.
• 7—Sets the network control precedence.

Default Configuration

There is no default configuration for this command.

Command Mode

Route Map mode

User Guidelines

The set ip precedence clause may be combined with set ip next-hop or set ip default next-hop clause in a route map.

Example

console(config-route-map)#set ip precedence 5
**show ip brief**

Use the `show ip brief` command to display all the summary information of the IP.

**Syntax**

`show ip brief [vrf vrf-name]`

- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example**

The following example displays IP summary information.

```
console#show ip brief
Default Time to Live......................... 64
Routing Mode................................. Enabled
ICMP Rate Limit Interval....................... 1000 msec
ICMP Rate Limit Burst Size..................... 100 messages
ICMP Echo Replies............................ Enabled
ICMP Redirect Mode........................... Enabled
Maximum Next Hops............................ 16
```
**show ip interface**

Use the **show ip interface** command to display information about one or more IP interfaces. The output shows how each IP address was assigned.

**Syntax**

`show ip interface [vrf vrf-name] [type number]`

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- **type**—Interface type (loopback, out-of-band, or VLAN)
- **number**—Interface number. Valid only for loopback and VLAN types.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The Method field contains one of the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>The address is leased from a DHCP server.</td>
</tr>
<tr>
<td>Manual</td>
<td>The address is manually configured.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ip interface

Default Gateway................................. 0.0.0.0
```
**L3 MAC Address.................................** 001E.C9DE.B546

**Routing Interfaces:**

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>IP Address</th>
<th>IP Mask</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vl1</td>
<td>Down</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>None</td>
</tr>
<tr>
<td>Vl2</td>
<td>Up</td>
<td>unnumbered</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

console#

cconsole#show ip interface vlan 1

Routing interface status....................... Up
Unnumbered - numbered interface............... Loopback 1
Unnumbered - gratuitous ARP accept............. Enable
Method......................................... None
Routing Mode................................... Enable
Administrative Mode............................ Enable
Forward Net Directed Broadcasts................. Disable
Proxy ARP...................................... Enable
Local Proxy ARP................................ Disable
Active State................................... Inactive
MAC Address.................................... 001E.C9DE.B546
Encapsulation Type............................. Ethernet
IP MTU......................................... 1500
Bandwidth...................................... 10000 Kbps
Destination Unreachables....................... Enabled
ICMP Redirects.................................. Enabled

**show ip policy**

Use the `show ip policy` command to display the route maps used for policy based routing on the router interfaces.

**Syntax**

`show ip policy map-name`

- **map-name**—The name of a specific route map.

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
```console
console#show ip policy
Interface                      Route map
Vl10                           pbr-map
```

**show ip protocols**

Use the `show ip protocols` command to display a summary of the configuration and status for each unicast routing protocol. The command lists all supported routing protocols, regardless of whether they are currently configured or enabled.

**Syntax**
```
show ip protocols [vrf vrf-name]
```
- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The VRF identified in the parameter must have been previously created or an error is returned.
The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The command displays the following information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BGP Section:</strong></td>
<td></td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>BGP.</td>
</tr>
<tr>
<td>Router ID</td>
<td>The router ID configured for BGP.</td>
</tr>
<tr>
<td>Local AS Number</td>
<td>The AS number that the local router is in.</td>
</tr>
<tr>
<td>BGP Admin Mode</td>
<td>Whether BGP is globally enabled or disabled.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an internal or external BGP route.</td>
</tr>
<tr>
<td>Distance</td>
<td>The default administrative distance (or route preference) for external,</td>
</tr>
<tr>
<td></td>
<td>internal, and locally-originated BGP routes. The table that follows lists</td>
</tr>
<tr>
<td></td>
<td>ranges of neighbor addresses that have been configured to override the</td>
</tr>
<tr>
<td></td>
<td>default distance with a neighbor-specific distance. If a neighbor’s address</td>
</tr>
<tr>
<td></td>
<td>falls within one of these ranges, routes from that neighbor are assigned</td>
</tr>
<tr>
<td></td>
<td>the configured distance. If a prefix list is configured, then the</td>
</tr>
<tr>
<td></td>
<td>distance is only assigned to prefixes from the neighbor that are</td>
</tr>
<tr>
<td></td>
<td>permitted by the prefix list.</td>
</tr>
<tr>
<td>Prefix List In</td>
<td>The global prefix list used to filter inbound routes from all neighbors.</td>
</tr>
<tr>
<td>Prefix List Out</td>
<td>The global prefix list used to filter outbound routes to all neighbors.</td>
</tr>
<tr>
<td>Neighbors</td>
<td>A list of configured neighbors and the inbound and outbound policies</td>
</tr>
<tr>
<td></td>
<td>configured for each.</td>
</tr>
<tr>
<td><strong>OSPFv2 Section</strong></td>
<td></td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>OSPFv2.</td>
</tr>
<tr>
<td>Router ID</td>
<td>The router ID configured for OSPFv2.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Whether OSPF is enabled or disabled globally.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an OSPF route.</td>
</tr>
<tr>
<td>Routing for</td>
<td>The address ranges configured with an OSPF network command.</td>
</tr>
<tr>
<td>Networks</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Distance</td>
<td>The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether OSPF is configured to originate a default route.</td>
</tr>
<tr>
<td>Always</td>
<td>Whether default advertisement depends on having a default route in the common routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric configured to be advertised with the default route.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>The metric type to advertise for redistributed routes of this type.</td>
</tr>
<tr>
<td>Redist Source</td>
<td>The type of routes OSPF is redistributing.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric to advertise for redistributed routes of this type.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>The metric type to advertise for redistributed routes of this type.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.</td>
</tr>
<tr>
<td>Dist List</td>
<td>A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.</td>
</tr>
<tr>
<td>Number of Active Areas</td>
<td>The number of OSPF areas with at least one interface running on this router. Also broken down by area type.</td>
</tr>
<tr>
<td>ABR Status</td>
<td>The number of OSPF areas with at least one interface running on this router. Also broken down by area type.</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.</td>
</tr>
</tbody>
</table>

**RIP Section**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP Admin Mode</td>
<td>Whether RIP is globally enabled.</td>
</tr>
<tr>
<td>Split Horizon Mode</td>
<td>Whether RIP advertises routes on the interface where they were received.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>The metric assigned to redistributed routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether this router is originating a default route.</td>
</tr>
<tr>
<td>Distance</td>
<td>The administrative distance for RIP routes.</td>
</tr>
</tbody>
</table>
**Example**

The following shows example CLI display output for the command.

```console
console# show ip protocols
Routing Protocol......................... BGP
Router ID................................ 6.6.6.6
Local AS Number.......................... 65001
BGP Admin Mode............................ Enable
Maximum Paths............................. Internal 32, External 32

Distance................................. Ext 20 Int 200 Local 200
Address         Wildcard     Distance   Pfx List
-------         --------      --------   -------
172.20.0.0      0.0.255.255   40        None
172.21.0.0      0.0.255.255   45         1

Prefix List In.......................... PfxList1
Prefix List Out.......................... None

Neighbors:
172.20.1.100
   Filter List In........................ 1
   Filter List Out....................... 2
   Prefix List In........................ PfxList2
   Prefix List Out....................... PfxList3
   Route Map In.......................... rmapUp
   Route Map Out......................... rmapDown
172.20.5.1
   Prefix List Out....................... PfxList12

Routing Protocol......................... OSPFv2
Router ID................................ 6.6.6.6
OSPF Admin Mode.......................... Enable
Maximum Paths............................ 32
Routing for Networks...................... 172.24.0.0 0.0.255.255 area 0
                                                10.0.0.0 0.255.255.255 area 1
                                                192.168.75.0 0.0.0.255 area 2
Distance.................................. Intra 110 Inter 110 Ext 110
Default Route Advertise................... Disabled
Always................................... FALSE
Metric................................... Not configured
Metric Type.............................. External Type 2
```

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interfaces where RIP is enabled and the version sent and accepted on each interface.</td>
</tr>
</tbody>
</table>
show ip route

Use the show ip route command to display the current state of the routing table. The output of the command also displays the IPv4 address of the default gateway and the default route associated with the gateway.

This command deprecates the show ip route connected command.

**Syntax**

```
show ip route [[ip-address [mask | prefix-length] [longer-prefixes] [vrf vrf-name] [static]]
```

- **ip-address**—Specifies the network for which the route is to be displayed and displays the best matching route for the address.
- **mask**—Subnet mask of the IPv4 address in dotted quad notation.
- **prefix-length**—Length of prefix, in bits. Must be preceded with a forward slash (/). (Range: 0-32 bits.)
- **longer-prefixes**—Indicates that the ip-address and subnet-mask pair becomes the prefix, and the command displays the routes to the addresses that match that prefix.
• vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

• static—Display statically configured routes.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

If the subnet mask is specified, then only routes with an exact match are displayed. For example:

```
show ip route 192.168.2.0 /24
```

If only an IP address is specified, the best route for the IP address is displayed. For example:

```
show ip route 192.168.2.0
```

If the `longer-prefixes` option is specified, then the subnets within an aggregate are displayed. For example:

```
show ip route 192.168.2.0 /23 longer-prefixes
```

The numbers in the brackets indicate the route preference (administrative distance) and metric respectively. The metric is specific to the originating protocol. Connected routes have a preference of 0 and static routes have a preference of 1.

**Example**

The following example displays the IPv4 address of the default gateway and the default route associated with the gateway.

```
console#show ip route
```
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, E - Externally Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
S U - Unnumbered Peer, L - Leaked Route, T - Truncated ECMP Route
* Indicates the best (lowest metric) route for the subnet.

C  3.0.0.0/24 [0/0] directly connected, Vl10
S U  6.1.0.6/32 [0/0] via Vl20
S U  6.2.0.6/32 [0/0] via Vl20

The following example shows an ECMP route with only one path.

console#show ip route summary

Connected Routes............................... 4
Static Routes.................................. 0
Kernel Routes.................................. 0
Unnumbered Peer Routes......................... 0
RIP Routes..................................... 0
BGP Routes..................................... 0
  External..................................... 0
  Internal..................................... 0
  Local........................................ 0
OSPF Routes..................................... 320
  Intra Area Routes............................ 0
  Inter Area Routes............................ 320
  External Type-1 Routes....................... 0
  External Type-2 Routes....................... 0
Reject Routes.................................. 0
Total routes................................... 324

Best Routes (High)............................. 324 (644)
Alternate Routes............................... 0
Leaked Routes.................................. 0
RFC5549 Routes - IPv4 with IPv6 nexthop..... 0
Route Adds..................................... 1629
Route Modifies................................. 1144
Route Deletes.................................. 1305
Unresolved Route Adds.......................... 0
Invalid Route Adds............................. 0
Failed Route Adds.............................. 0
Failed Kernel Route Adds....................... 0
Hardware Failed Route Adds..................... 0
Reserved Locals................................ 0

Unique Next Hops (High)....................... 68 (132)
Next Hop Groups (High)......................... 299 (599)
ECMP Groups (High).............................. 290 (585)
ECMP Routes.................................... 256
Truncated ECMP Routes......................... 34
ECMP Retries.................................. 26400
show ip route static

Use the show ip route static command to display the statically configured routes, whether they are reachable or not.

**Syntax**

show ip route static [name]

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

Use the optional name parameter to display the route name in addition to the other information displayed

**Example**

    console#show ip route static
    Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
    B - BGP Derived, E - Externally Derived, IA - OSPF Inter Area
    E1 - OSPF External Type 1, E2 - OSPF External Type 2
    N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
    S U - Unnumbered Peer, L - Leaked Route
    No default gateway is configured.
    S 10.0.0.0/8 [1/0] via Vl10
    S U 6.1.0.6/32 [0/0] via Vl120
    S U 6.2.0.6/32 [0/0] via Vl120

**show ip route preferences**

Use the show ip route preferences command to display the default route preference value for each origin.
Syntax
show ip route preferences

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. This command displays the route preferences for each possible route origin.

Example
The following example displays IP route preferences.

console#show ip route preferences
Local.......................................... 0
Static........................................ 1
OSPF Intra-area routes.......................... 110
OSPF Inter-area routes.......................... 110
OSPF External routes.......................... 110
RIP........................................... 120
BGP External.................................. 20
BGP Internal.................................. 200
BGP Local.................................... 200
Configured Default Gateway.................. 253
DHCP Default Gateway......................... 254

show ip route summary
Use the show ip route summary command to display the routing table summary, including best and non-best routes.

Syntax
show ip route summary [best]
• best—Shows the number of best routes. To include the count of all routes, do not use this optional parameter.
Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the IP route summary.

```
console#show ip route summary

Connected Routes............................... 4
Static Routes.................................. 0
Kernel Routes.................................. 0
Unnumbered Peer Routes........................ 0
RIP Routes..................................... 0
BGP Routes..................................... 0
  External..................................... 0
  Internal..................................... 0
  Local........................................ 0
OSPF Routes................................... 320
  Intra Area Routes............................ 0
  Inter Area Routes........................... 320
  External Type-1 Routes...................... 0
  External Type-2 Routes...................... 0
Reject Routes.................................. 0
Total routes................................... 324

Best Routes (High)............................. 324 (644)
Alternate Routes............................... 0
Leaked Routes.................................. 0
RFC5549 Routes - IPv4 with IPv6 nexthop...... 0
Route Adds...................................... 1629
Route Modifies................................ 1144
Route Deletes.................................. 1305
Unresolved Route Adds.......................... 0
Invalid Route Adds............................. 0
Failed Route Adds............................. 0
Failed Kernel Route Adds...................... 0
Hardware Failed Route Adds.................... 0
Reserved Locals............................... 0
```
show ip traffic

Use the show ip traffic command to display IP statistical information of the software IP stack. Refer to RFC 1213 for more information about the fields that are displayed.

**Syntax**

```
show ip traffic [vrf vrf-name]
```

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command displays statistics for the software IP stack, not the hardware routing information.

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.
Example

The following example displays IP route preferences.

console>show ip traffic
IpInReceives................................... 24002
IpInHdrErrors.................................. 1
IpInAddrErrors................................. 925
IpForwDatagrams............................... 0
IpInUnknownProtos............................. 0
IpInDiscards................................... 0
IpInDelivers.................................. 18467
IpOutRequests.................................. 295
IpOutDiscards.................................. 0
IpOutNoRoutes.................................. 0
IpReasmTimeout................................. 0
IpReasmReqds................................... 0
IpReasmOKs..................................... 0
IpReasmFails................................... 0
IpFragOKs...................................... 0
IpFragFails.................................... 0
IpFragCreates.................................. 0
IpRoutingDiscards............................. 0
IcmpInMsgs..................................... 3
IcmpInErrors................................... 0
IcmpInDestUnreachs............................. 0
IcmpInTimeExcds............................... 0
IcmpInParmProbs............................... 0
IcmpInSrcQuenches............................. 0
IcmpInRedirects............................... 0
IcmpInEchos.................................. 3
IcmpInEchoReps............................... 0
IcmpInTimestamps.............................. 0
IcmpInTimestampReps........................... 0
IcmpInAddrMasks............................... 0
IcmpOutMsgs.................................... 3
IcmpOutErrors.................................. 0
IcmpOutDestUnreaches.......................... 0
IcmpOutTimeExcds.............................. 0
IcmpOutParmProbs.............................. 0
IcmpOutSrcQuenches............................ 0
IcmpOutRedirects.............................. 0
IcmpOutEchos.................................. 3
IcmpOutEchoReps.............................. 3
IcmpOutTimestamps............................. 0
IcmpOutTimestampReps.......................... 0
IcmpOutAddrMasks.............................. 0
**show ip vlan**

Use the `show ip vlan` command to display the VLAN routing information for all VLANs with routing enabled.

**Syntax**

```
show ip vlan
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays VLAN routing information.

```
console#show ip vlan
MAC Address used by Routing VLANs: 00:00:00:01:00:02
VLAN ID IP Address       Subnet Mask
------- --------------- ---------------
  10    0.0.0.0       0.0.0.0
  20    0.0.0.0       0.0.0.0
```

**show route-map**

Use this command to display the route maps.

**Syntax**

```
show route-map map-name
```

**Default Configuration**

This command has no default configuration.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

For each route map, the match count is shown in terms of number of packets and number of bytes. This counter displays the match count in packets and bytes when a route map is applied. When a route map is created/removed from interface, this count is shown as zero. The following is an example of the behavior of counters as well as how they are displayed when a route-map is applied and removed from interface:

```console
console# show route-map test
route-map test, permit, sequence 10
  Match clauses:
    ip address prefix-lists: orange
  Set clauses:
    set metric 50

console #show ip policy

Interface          Route-Map
---------------  -----------------------------------------

console #show route-map simplest

route-map simplest permit 10
  Match clauses:
    ip address (access-lists) : 1
  Set clauses:
    ip next-hop 3.3.3.3
    ip precedence 3
Policy routing matches: 0 packets, 0 bytes

route-map simplest permit 20
  Match clauses:
    ip address (access-lists) : 1
  Set clauses:
    ip default next-hop 4.4.4.4
    ip precedence 4
Policy routing matches: 0 packets, 0 bytes

route-map simplest permit 30
  Match clauses:
  Set clauses:
    interface null0
Policy routing matches: 0 packets, 0 bytes
```
console #configure
console (Config)#interface Te1/0/2
console (config-if-Te1/0/2)#ip policy simplest
console (config-if-Te1/0/2)#show route-map simplest
route-map simplest permit 10
    Match clauses:
        ip address (access-lists) : 1
    Set clauses:
        ip next-hop 3.3.3.3
        ip precedence 3
Policy routing matches: 5387983 packets, 344831232 bytes
route-map simplest permit 20
    Match clauses:
        ip address (access-lists) : 1
    Set clauses:
        ip default next-hop 4.4.4.4
        ip precedence 4
Policy routing matches: 0 packets, 0 bytes
route-map simplest permit 30
    Match clauses:
    Set clauses:
        interface null0
Policy routing matches: 0 packets, 0 bytes
console (config-if-Te1/0/2)# no ip policy simplest
console (config-if-Te1/0/2)# exit
console (config)# exit
console # show ip policy

<table>
<thead>
<tr>
<th>Interface</th>
<th>Route-Map</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

console #
console(route-map)#show route-map

route-map "d3" permit 10
    Match clauses:
ip address prefix-list a1
as-path 1
community s1 exact-match
Set clauses:
  metric 23
  local-preference 34
  as-path prepend 2 3 4 5 6
  comm-list d1 delete
  community no-export
ipv6 next-hop aa::bb
Policy routed: 0 packets, 0 bytes

The following example shows a route map test1 that is configured with extended community attributes:

crsole# show route-map test
route-map test1, permit, sequence 10
  Match clauses:
    extended community list1
  Set clauses:
    extended community RT:1:100 RT:2:200

show routing heap summary

Use the show routing heap summary command to display a summary of the memory allocation from the routing heap. The routing heap is a section of memory set aside when the system boots for use by the routing applications.

Syntax

show routing heap summary

Default Configuration

This command has no default setting.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The command displays the following information.
### Examples

The following shows example CLI display output for the command.

```plaintext
console# show routing heap summary

Heap Size.......................  92594000 bytes
Memory In Use...................   149598 bytes (0%)
Memory on Free List.............    78721 bytes (0%)
Memory Available in Heap........ 92365249 bytes (99%)
In Use High Water Mark..........   210788 bytes (0%)
```
IPv6 Routing Commands

The Dell Network N1500/N2000/N2100-ON series supports limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

The IPv6 version of the routing table manager provides a repository for IPv6 routes learned by dynamic routing protocols or static configuration. RTO6 manages dynamic and static IPv6 routes, redistributes routes to registered protocols, supports ECMP routes, and supports multiple routes to the same destination, sorted by preference. IPv6 routing only operates over VLAN interfaces.

IPv6 Limitations & Restrictions

The following limitations apply:

• IPSec support is not available.

• The DHCPv6 server does not support stateful address configuration.

• Automated router renumbering is not supported.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>ipv6 nd dad attempts</td>
</tr>
<tr>
<td>clear ipv6 statistics</td>
<td>ipv6 nd ra hop-limit unspecified</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>ipv6 nd managed-config-flag</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>ipv6 nd ns-interval</td>
</tr>
<tr>
<td>ipv6 hop-limit</td>
<td>ipv6 nd nud max-multicast-solicits</td>
</tr>
<tr>
<td></td>
<td>show ipv6 mld host-proxy groups</td>
</tr>
<tr>
<td></td>
<td>show ipv6 mld host-proxy groups detail</td>
</tr>
<tr>
<td></td>
<td>show ipv6 mld host-proxy interface</td>
</tr>
<tr>
<td></td>
<td>show ipv6 mld traffic</td>
</tr>
<tr>
<td></td>
<td>show ipv6 nd raguard policy</td>
</tr>
</tbody>
</table>
clear ipv6 neighbors

Use the clear ipv6 neighbors command to clear all entries in the IPv6 neighbor table or an entry on a specific interface.

**Syntax**

clear ipv6 neighbors [vlan vlan-id]

- **vlan-id** — Valid VLAN ID.

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged Exec mode.

User Guidelines
This command has no user guidelines.

Example
The following example clears all entries in the IPv6 neighbor table.
console(config)#clear ipv6 neighbors

clear ipv6 statistics

Use the clear ipv6 statistics command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the show ipv6 traffic command.

Syntax
clear ipv6 statistics [vlan vlan-id | tunnel tunnel-id | loopback loopback-id]
• vlan-id — Valid VLAN ID.
• tunnel-id — Tunnel identifier. (Range: 0-7)
• loopback-id — Loopback identifier. (Range: 0-7)

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode.

User Guidelines
This command has no user guidelines.

Example
The following example clears IPv6 statistics for VLAN 11.
console(config)#clear ipv6 statistics vlan 11
**ipv6 address**

Use the `ipv6 address` command in Interface Configuration mode to configure an IPv6 address on an interface (including VLAN, tunnel and loopback interfaces) and to enable IPv6 processing on this interface. Multiple globally reachable addresses can be assigned to an interface by using this command. There is no need to assign a link-local address by using this command since one is automatically created. IPv6 addresses can be expressed in eight blocks. Also of note is that instead of a period, a colon separates each block. For simplification, leading zeros of each 16-bit block can be omitted. One sequence of 16-bit blocks containing only zeros can be replaced with a double colon “::”, but not more than one at a time (otherwise it is no longer a unique representation).

Dropping zeros: 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1
Local host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::
The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

**Syntax**

`ipv6 address prefix/prefix-length [eui64]`

`no ipv6 address [prefix/prefix-length] [eui64]`

- **prefix** — Consists of the bits of the address to be configured.
- **prefix-length** — Designates how many of the high-order contiguous bits of the address make up the prefix.
- **eui64** — The optional eui-64 field designates that IPv6 processing on the interfaces is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, the value of prefix_length must be 64 bits.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.
User Guidelines
This command has no user guidelines.

Example
The following example configures an IPv6 address and enables IPv6 processing.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 address 2020:1::1/64
```

ipv6 enable

Use the `ipv6 enable` command in VLAN Interface Configuration mode to enable IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address. Command execution automatically configures the interface with a link-local address. The command is not required if an IPv6 global address is configured on the interface.

Syntax
ipv6 enable
no ipv6 enable

Default Configuration
Disabled is the default configuration.

Command Mode
Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines
This command has no user guidelines.

Example
The following example enables IPv6 routing, which has not been configured with an explicit IPv6 address.

```
console(config)#vlan 15
console(config-vlan)#interface vlan 15
```
ipv6 hop-limit

Use the `ipv6 hop-limit` command to configure the hop limit used in IPv6 PDUs originated by the router. Use the `no` form of the command to return the hop limit to the default setting.

**Syntax**

```
ipv6 hop-limit count
no ipv6 hop-limit
```

- count—The number of hops before the PDU expires (Range 1-255).

**Default Configuration**

The default count is “not configured.”

**Command Mode**

Global Configuration

**User Guidelines**

The default “not configured” sends a value of 0 in router advertisements and a value of 64 in packets originated by the router. This is not the same as configuring a hop limit of 64.

ipv6 host

The `ipv6 host` command is used to define static host name-to-ipv6 address mapping in the host cache.

**Syntax**

```
ipv6 host name ipv6-address
no ipv6 host name
```

- name — Host name.
- ipv6-address — IPv6 address of the host.
Default Configuration
No IPv6 hosts are defined.

Command Mode
Global Configuration mode.

User Guidelines
This command has no user guidelines.

Example
console(config)#ipv6 host Dell 2001::DB8:0

ipv6 icmp error-interval
Use the icmp error-interval command to limit the rate at which ICMP error messages are sent. The rate limit is configured as a token bucket with two configurable parameters: Burst-size and burst interval. Use the no form of this command to return burst-interval and burst-size to their default values. To disable ICMP rate limiting, set burst-interval to zero.

Syntax
ipv6 icmp error-interval burst-interval [ burst-size ]
no ipv6 icmp error-interval

• burst-interval — How often the token bucket is initialized (Range: 0–2147483647 milliseconds).
• burst-size — The maximum number of messages that can be sent during a burst interval (Range: 1–200).

Default Configuration
Rate limiting is enabled by default.
The default burst-interval is 1000 milliseconds.
The default burst-size is 100 messages.

Command Mode
Global Configuration mode
User Guidelines
There are no user guidelines for this command.

Example
```
console(config)#ipv6 icmp error-interval 2000 20
```

**ipv6 mld last-member-query-count**

The `ipv6 mld last-member-query-count` command sets the number of listener-specific queries sent before the router assumes that there are no local members on the interface. Use the “no” form of this command to set the last member query count to the default.

**Syntax**
```
ipv6 mld last-member-query-count last-member-query-count
no ipv6 mld last-member-query-count
```

- `last-member-query-count` — Query count (Range: 1–20).

**Default Configuration**
The default last member query count is 2.

**Command Mode**
Interface Configuration (VLAN) mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-if-vlan3)#ipv6 mld last-member-query-count 5
```
**ipv6 mld last-member-query-interval**

The `ipv6 mld last-member-query-interval` command sets the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group-specific queries sent out of this interface. Use the “no” form of this command to set the last member query interval to the default.

**Syntax**

```
ipv6 mld last-member-query-interval last-member-query-interval
no ipv6 mld last-member-query-interval
```

- `last-member-query-interval` — The last member query interval (Range: 0–65535 milliseconds).

**Default Configuration**

The default last member query interval is 1 second.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config-if-vlan3)#ipv6 mld last-member-query-interval 5000
```

**ipv6 mld host-proxy**

This command enables MLD and MLD Proxy on the specified interface. PIM and DVMRP are not compatible with MLD proxy. Disable PIM/DVMRP before enabling MLD proxy.

Multicast routing must be enabled for the MLD proxy service to become operationally enabled.

Also, ensure that there are no other multicast routing protocols enabled on the router and that IP multicast routing is globally enabled. Use the “no” form of this command to disable MLD Proxy globally.
Syntax
ipv6 mld host-proxy [interface vlan-id]
no ipv6 mld host-proxy [interface vlan-id]

Default Configuration
MLD Proxy is disabled by default.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-if-vlan3)#ipv6 mld host-proxy

ipv6 mld host-proxy reset-status

Use the ipv6 mld host-proxy reset-status command to reset the host interface status parameters of the MLD Proxy router. This command is only valid when MLD Proxy is enabled on the interface.

Syntax
ipv6 mld host-proxy reset-status

Command Mode
Interface Configuration (VLAN) mode.

Default Configuration
There is no default configuration for this command.

User Guidelines
There are no user guidelines for this command.
Example
console(config-if-vlan3)#ipv6 mld host-proxy reset-status

**ipv6 mld host-proxy unsolicit-rprt-interval**

Use the `ipv6 mld host-proxy unsolicit-rprt-interval` command to set the unsolicited report interval for the MLD Proxy router. This command is only valid when MLD Proxy is enabled on the interface. Use the “no” form of this command to reset the MLD Proxy router's unsolicited report interval to the default value.

**Syntax**

```
ipv6 mld host-proxy unsolicit-report-interval interval
no ipv6 mld host-proxy unsolicit-report-interval
```

- interval — The interval between unsolicited reports (Range: 1–260 seconds).

**Default Configuration**

The unsolicited report interval is 1 second by default.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines

**Example**

```
console(config-if-vlan3)#ipv6 mld host-proxy unsolicit-rprt-interval 10
```

**ipv6 mld query-interval**

The `ipv6 mld query-interval` command sets the MLD router's query interval for the interface. The query-interval is the amount of time between the general queries sent when the router is querying on that interface. Use the “no” form of this command to set the query interval to the default.
Syntax
ipv6 mld query-interval query-interval
no ipv6 mld query-interval
  • query-interval — Query interval (Range: 1–3600).

Default Configuration
The default query interval is 125 seconds.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-if-vlan3)#ipv6 mld query-interval 130

ipv6 mld query-max-response-time
The ipv6 mld query-max-response-time command sets MLD query maximum response time for the interface. This value is used in assigning the maximum response time in the query messages that are sent on that interface. Use the “no” form of this command to set the maximum query response time to the default.

Syntax
ipv6 mld query-max-response-time query-max-response-time
no ipv6 mld query-max-response-time
  • query-max-response-time — Maximum query response time (Range: 1–65535 milliseconds).

Default Configuration
The default query maximum response time is 10 seconds.
**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-if-vlan3)#ipv6 mld query-max-response-time 4500
```

**ipv6 nd dad attempts**
Use the `ipv6 nd dad attempts` command in Interface Configuration mode to set the number of duplicate address detection probes transmitted while doing neighbor discovery. Duplicate address detection verifies that an IPv6 address on an interface is unique.

**Syntax**
```
ipv6 nd dad attempts value
no ipv6 nd dad attempts
```
- `value`—Probes transmitted. (Range: 0-600)

**Default Configuration**
The default value for attempts is 1.

**Command Mode**
Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets at 10 the number of duplicate address detection probes transmitted while doing neighbor discovery.
```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd dad attempts 10
```
ipv6 nd ra hop-limit unspecified

Use the `ipv6 nd ra hop-limit unspecified` command to configure the hop limit sent in router alert messages. Use the `no` form of the command to send the default hop limit of 64.

**Syntax**

```
ipv6 nd ra hop-limit unspecified
no ipv6 nd ra hop-limit unspecified
```

**Default Configuration**

The default TTL is 64.

**Command Mode**

Interface (VLAN) Configuration

**User Guidelines**

The TTL sent in router advertisements and neighbor discovery packets may be configured using the Global Configuration command `ipv6 hop-limit`.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra hop-limit unspecified
```

ipv6 nd managed-config-flag

Use the `ipv6 nd managed-config-flag` command in Interface Configuration mode to set the “managed address configuration” flag in router advertisements. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.
**Syntax**
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

**Default Configuration**
False is the default configuration.

**Command Mode**
Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**
This command has no user guidelines.

**Example**
In the following example, the end node uses DHCPv6.
```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd managed-config-flag
```

**ipv6 nd ns-interval**
Use the `ipv6 nd ns-interval` command in Interface Configuration mode to set the interval between router advertisements for advertised neighbor solicitations. An advertised value of 0 means the interval is unspecified.

**Syntax**
ipv6 nd ns-interval milliseconds
no ipv6 nd ns-interval

- milliseconds — Interval duration. (Range: 0, 1000–4294967295)

**Default Configuration**
0 is the default value for milliseconds.

**Command Mode**
Interface Configuration (VLAN, Tunnel, Loopback) mode
**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the interval between router advertisements for advertised neighbor solicitations at 5000 ms.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ns-interval 5000
```

**ipv6 nd nud max-multicast-solicits**

Configures the maximum number of multicast neighbor solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection). Use the `no` form of the command to reset the value to the default.

**Syntax**

```
ipv6 nd nud max-multicast-solicits num-solicits
no ipv6 nd nud max-multicast-solicits
```

- `num-solicits`—The maximum number of multicast Neighbor Solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection). The value ranges from 3 to 255. The default value is 3.

**Default Configuration**

The default number of multicast solicits is 3.

**Command Mode**

Global Configuration

**User Guidelines**

Increase this value when neighbors are not being discovered or large numbers of neighbors are present.

**Command History**

Introduced in version 6.2.0.1 firmware.
Example
console (config)#ipv6 nd nud max-multicast-solicits 5

**ipv6 nd nud max-unicast-solicits**

Configures the maximum number of unicast neighbor solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection). Use the no form of the command to reset the value to the default.

**Syntax**

ipv6 nd nud max-unicast-solicits num-solicits
no ipv6 nd nud max-unicast-solicits

num-solicits—The maximum number of unicast Neighbor Solicitations sent during neighbor resolution or during NUD (neighbor unreachability detection). The value ranges from 3 to 10. The default value is 3.

**Default Configuration**

The default number of solicits is 3.

**Command Mode**

Global Configuration

**User Guidelines**

Increase this value when neighbors are not being discovered or large numbers of neighbors are present.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

console (config)#ipv6 nd nud max-unicast-solicits 5
**ipv6 nd nud retry**

This command configures the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachability detection) following the exponential backoff algorithm. Use the `no` form of the command to return the backoff multiple to the default.

**Syntax**

ipv6 nd nud retry backoff-multiple

no ipv6 nd nud retry

- backoff-multiple—The value ranges from 1 to 5. The next timeout value is clamped at a maximum value of 60 seconds if the result of the exponential back-off calculation is greater than 60 seconds.

**Default Configuration**

The default exponent is 1.

**Command Mode**

Global Configuration

**User Guidelines**

Once the neighbor is resolved and added in the hardware, traffic is continuously forwarded by the router using neighbor entry. The neighbor entry in the cache transitions to the STALE state after the effective STALE timeout value (a random value between 15 and 45 seconds per RFC 2461).

To bridge the gap between the neighbor discovery state and the neighbor cache state, the application periodically iterates through the STALE entries and triggers NUD on those entries to detect any address/station movements or MAC address changes.

When NUD is triggered, neighbor solicitation PROBE packets (unicast and multicast) are sent periodically, separated by exponential binary values instead of the normal 1 second interval. This ensures that when the network (not just our router but more routers in the network) is congested, the NUD process for the existing STALE entries takes enough time before ultimately removing the cache entry through garbage collection. Without the
exponential backoff timing for retransmissions, there is a higher probability that the cache entry is removed resulting in the disruption of the existing traffic.

Another significant benefit of delayed neighbor solicitation retransmission is higher robustness against transient failures, such as spanning tree re-convergence and other layer 2 issues that can take many seconds to resolve.

The exponential back-off calculation is

next retransmission timer =
(BACKOFF_MULTIPLE ^ solicit_attempt_num) * RETRANS_TIMER + jittered value.

The exponential backoff algorithm complies with draft-ietf-6man-impatient-nud-02.

Increase this value when large numbers of neighbors are present or when neighbors are not being discovered due to network events like spanning-tree re-convergence.

Command History

Introduced in version 6.2.0.1 firmware.

Example

console (config)#ipv6 nd nud retry 5

ipv6 nd other-config-flag

Use the ipv6 nd other-config-flag command in Interface Configuration mode to set the “other stateful configuration” flag in router advertisements sent from the interface.

Syntax

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Default Configuration

False is the default configuration.
**Command Mode**
Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets to true the “other stateful configuration” flag in router advertisements

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd other-config-flag
```

**ipv6 nd prefix**
Use the `ipv6 nd prefix` command to configure parameters associated with prefixes that the router advertises in its router advertisements.

**Syntax**
```
ipv6 nd prefix ipv6-prefix/prefix-length [{valid-lifetime | infinite} {preferred-lifetime | infinite}] [no-autoconfig] [off-link]
```

no ipv6 nd prefix ipv6-prefix/prefix-length
- `ipv6-prefix`—IPv6 prefix.
- `prefix-length`—IPv6 prefix length.
- `valid-lifetime`—Valid lifetime of the router in seconds. (Range: 0–4294967295 seconds.)
- `infinite`—Indicates lifetime value is infinite.
- `preferred-lifetime`—Preferred lifetime of the router in seconds. (Range: 0–4294967295 seconds.)
- `no-autoconfig`—Do not use Prefix for autoconfiguration.
- `off-link`—Do not use Prefix for onlink determination.

**Default Configuration**
604800 seconds is the default value for valid-lifetime, 2592000 seconds for preferred lifetime.
**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the ipv6 address interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the `ipv6 nd prefix` command to configure these values.

The ipv6 nd prefix command will allow you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the `ipv6 address` command. Prefixes specified using ipv6 nd prefix without an associated interface address will not be included in RAs and will not be committed to the device configuration.

**Example**

The following example sets the IPv6 prefixes to include in the router advertisement.

```console
console(config)#interface vlan 11
console(config-if-vlan11)#ipv6 nd prefix 2020:1::1/64
```

**ipv6 nd raguard attach-policy**

Use this command to enable RA Guard policy on an interface. Use the `no` form of the command to disable RA-Guard.

**Syntax**

- `ipv6 nd raguard attach-policy`
- `no ipv6 nd raguard attach-policy`

**Default Configuration**

By default, no RA guard policies are applied to any interface.
**Command Mode**
Interface Configuration (Ethernet, port-channel)

**User Guidelines**
RA Guard drops all incoming IPv6 router advertisement and router redirect messages.
RA Guard may be configured on L2 or L3 interfaces.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
The following example configures an unnamed RA Guard policy to drop all RA advertisements and router redirect messages on IPv6 routing enabled interface Gi1/0/1 (VLAN 10).

```
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface vlan 10
console(config-if-vlan10)#ipv6 enable
console(config-if-vlan10)#exit
console(config)#ipv6 unicast-routing
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport access vlan 10
console(config-if-Gi1/0/1)#exit
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#ipv6 nd raguard attach-policy
```

**ipv6 nd ra-interval**
Use the `ipv6 nd ra-interval` command in Interface Configuration mode to set the transmission interval between router advertisements.

**Syntax**
- `ipv6 nd ra-interval` maximum minimum
- `no ipv6 nd ra-interval`
  - maximum — The maximum interval duration (Range: 4–1800 seconds).
  - minimum — The minimum interval duration (Range: 3 – (0.75 * maximum) seconds).
**Default Configuration**

600 is the default value for seconds.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**

The minimum interval cannot be larger than 75% of the maximum interval.

**Example**

The following example sets the transmission interval between router advertisements at 1000 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra-interval 1000
```

**ipv6 nd ra-lifetime**

Use the `ipv6 nd ra-lifetime` command in Interface Configuration mode to set the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.

**Syntax**

```
ipv6 nd ra-lifetime seconds
no ipv6 nd ra-lifetime
```

- **seconds** — Lifetime duration. The value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000 seconds. A value of zero means this router is not to be used as the default router. (Range: 0-9000)

**Default Configuration**

1800 is the default value for seconds.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode
User Guidelines

This command has no user guidelines.

Example

The following example sets at 1000 seconds the value that is placed in the Router Lifetime field of the router advertisements.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra-lifetime 1000
```

ipv6 nd reachable-time

Use the `ipv6 nd reachable-time` command in Interface Configuration mode to set the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.

Syntax

```
ipv6 nd reachable-time milliseconds
no ipv6 nd reachable-time
```

- milliseconds — Reachable-time duration. A value of zero means the time is unspecified by the router. (Range: 0-3600000 milliseconds)

Default Configuration

The default value for neighbor discovery reachable times is 0 milliseconds.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the router advertisement time at 5000 milliseconds to consider a neighbor reachable after neighbor discovery confirmation.

```
console(config)#interface vlan 15
```
**ipv6 nd suppress-ra**

Use the `ipv6 nd suppress-ra` command in Interface Configuration mode to suppress router advertisement transmission on an interface.

**Syntax**

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example suppresses router advertisement transmission.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd suppress-ra
```

**ipv6 redirect**

Use the `ipv6 redirect` command to enable sending IPv6 ICMP redirect messages to peers/hosts when a better first-hop node exists on the path to a destination. Use the `no` form of the command to disable IPv6 ICMP redirects.

**Syntax**

ipv6 redirect
no ipv6 redirect
**Default Configuration**
IPv6 ICMP redirects are enabled by default.

**Command Mode**
Interface VLAN Configuration mode

**User Guidelines**
In general, an IPv6 ICMP redirect is sent if:

- The packet is not addressed to the router.
- The packet will be forwarded over the interface on which it was received.
- The router determines that a better first-hop resides on the same VLAN as the source of the packet.
- The source address of the received packet is a link-local or global IPv6 address of a neighbor on the VLAN.
- Using the `no` form of the command to disable IPv6 ICMP redirects.

**Command History**
Command introduced in version 6.5 firmware.

**Example**
This example disables sending of IPv6 ICMP redirects on VLAN 6.

```
console(config-if-vlan6)# no ipv6 redirects
```

**ipv6 route**
Use the `ipv6 route` command in Global Configuration mode to configure an IPv6 static route. Use the `no` form of the command to remove a preference, an individual next hop, or all next hops for a route. Using the `no ipv6 route distance` form causes the system to use the system default administrative distance.

**Syntax**
```
ipv6 route distance
```
ipv6 route ipv6-prefix/prefix-length {ipv6-address | interface-type ipv6-address} [preference]

no ipv6 route ipv6-prefix/prefix-length ipv6-address preference

no ipv6 route ipv6-prefix/prefix-length interface-type ipv6-address

no ipv6 route ipv6-prefix/prefix-length interface

- distance—The default administrative distance for static routes. (Range 1-255)
- ipv6-prefix—An IPv6 prefix representing the subnet that can be reached via the next-hop neighbor.
- prefix-length—The length of the IPv6 prefix — a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must separate the prefix from the prefix-length with no spaces on either side of the slash mark.
- interface-type—Distinguishes direct static routes from point-to-point and broadcast interfaces, and must be specified when using a link-local address as the next hop. Interface-type can be Null 0 or vlan plus vlan-id or tunnel plus tunnel-id.
- ipv6-address—The IPv6 address of the next hop neighbor.
- preference—The administrative distance the router uses to compare this route with routes from other route sources that have the same destination. (Range: 1-255)

Default Configuration

1 is the default value for preference.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configure an IPv6 static route.
**ipv6 route distance**

Use the `ipv6 route distance` command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The `ipv6 route` and `ipv6 route default` commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance is applied to static routes created after invoking the `ipv6 route distance` command.

**Syntax**

```
ipv6 route distance integer
no ipv6 route distance integer
```

- `integer` — Specifies the distance (preference) of an individual static route. (Range 1-255)

**Default Configuration**

Default value of integer is 1.

**Command Mode**

Global Configuration mode

**User Guidelines**

Lower route distance values are preferred when determining the best route.

**Example**

The following example sets the default distance to 80.

```
console(config)#ipv6 route distance 80
```
**ipv6 unicast-routing**

Use the `ipv6 unicast-routing` command in Global Configuration mode to enable forwarding of IPv6 unicast datagrams.

**Syntax**

ipv6 unicast-routing  
no ipv6 unicast-routing

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example globally enables IPv6 unicast datagram forwarding.

```
console(config)#ipv6 unicast-routing
console(config)#no ipv6 unicast-routing
```

**ipv6 unreachable**

Use the `ipv6 unreachable` command to enable the generation of ICMPv6 Destination Unreachable messages. Use the `no` form of this command to prevent the generation of ICMPv6 Destination Unreachable messages.

**Syntax**

ipv6 unreachable  
no ipv6 unreachable

**Default Configuration**

ICMPv6 Destination Unreachable messages are enabled by default.
**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config-if-vlan10)#ipv6 unreachables
```

### show ipv6 brief

Use the `show ipv6 brief` command to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

**Syntax**
```
show ipv6 brief
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.
```
console#show ipv6 brief
IPv6 Unicast Routing Mode.................... Enable
IPv6 Hop Limit............................... Unconfigured
ICMPv6 Rate Limit Error Interval............. 1000 msec
ICMPv6 Rate Limit Burst Size............... 100 messages
```
show ipv6 interface

Use the show ipv6 interface command to show the usability status of IPv6 interfaces. The output of the command includes the method of assignment for each IPv6 address that is either autoconfigured or leased from a DHCP server. Global addresses with no annotation are assumed to be manually configured.

Syntax

show ipv6 interface [brief] [loopback loopback-id | tunnel tunnel-id | vlan vlan-id [prefix]]

- loopback-id—Valid loopback interface ID
- tunnel-id—Valid tunnel interface ID
- vlan-id—Valid VLAN ID
- prefix—Display IPv6 Interface Prefix Information.

Default Configuration

Displays all IPv6 interfaces.

Command Mode

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines

The Method field contains one of the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>The IPv6 address is automatically generated using IPv6 auto address configuration (RFC 2462).</td>
</tr>
<tr>
<td>Config</td>
<td>The IPv6 address is manually configured.</td>
</tr>
<tr>
<td>DHCP</td>
<td>The IPv6 address is leased from a DHCP server.</td>
</tr>
<tr>
<td>TENT</td>
<td>Tentative address.</td>
</tr>
</tbody>
</table>
The long form of the command includes the same annotations and shows whether address autoconfiguration or DHCP client are enabled on the interface. When the interface acts as a host interface, the output also shows the default gateway on the interface, if one exists.

**Examples**

The following example shows the method of assignment for each IPv6 address that is either autoconfigured or leased from a DHCP server.

```
console#show ipv6 interface
Oper. Interface Mode IPv6 Address/Length
---------- -------- ---------------------------------
Vl3        Enabled  FE80::211:88FF:FE2A:3E3C/128
2033::211:88FF:FE2A:3E3C/64
Vl5        Enabled  FE80::211:88FF:FE2A:3E3C/128
2017::A42A:26DB:1049:43DD/128 [DHCP]
Vl7        Enabled  FE80::211:88FF:FE2A:3E3C/128
2001::211:88FF:FE2A:3E3C/64 [AUTO]
Vl9        Disabled FE80::211:88FF:FE2A:3E3C/128 [TENT]
```

The Method column shows one of the following values:

- **Auto** – The IPv6 address was automatically generated using IPv6 auto address configuration (RFC 2462)
- **Config** – The IPv6 address was manually configured.
- **DHCP** – The IPv6 address was leased from a DHCP server.
- **TENT** – Tentative address.

The following example displays the long form of the command, and indicates whether address autoconfiguration or DHCP client are enabled on the interface. When the interface acts as a host interface, the output also shows the default gateway on the interface, if one exists.

```
console#show ipv6 interface vlan2
IPv6 is enabled
IPv6 Prefix is ................................ FE80::211:88FF:FE2A:3E3C/128
2033::211:88FF:FE2A:3E3C/64 [DHCP]
Routing Mode................................... Enabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode................. Enabled
Bandwidth...................................... 100000 Kbps
Interface Maximum Transmit Unit.............. 1500
Router Duplicate Address Detection Transmits... 1
Address Autoconfigure Mode.................... Disabled
```
show ipv6 mld groups

The show ipv6 mld groups command is used to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on any interfaces, there is no group information to be displayed.

Syntax

show ipv6 mld groups {group-address | vlan vlan-id}

- group-address — The group address to display.
- vlan-id — A valid VLAN id.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following fields are displayed as a table when vlan vlan-id is specified:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of (*, G) entries</td>
<td>Displays the number of groups present in the MLD Table.</td>
</tr>
</tbody>
</table>
If `vlan` `vlan-id` is not specified, the following fields are displayed for each multicast group and each interface:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The address of the multicast group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the multicast group is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time elapsed in seconds since the multicast group has been known.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time left in seconds before the entry is removed from the MLD membership table of this interface.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP Address of the source of the last membership report received for this multicast group address on that interface.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>The filter mode of the multicast group on this interface. The values it can take are INCLUDE and EXCLUDE.</td>
</tr>
<tr>
<td>Compatibility Mode</td>
<td>The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.</td>
</tr>
<tr>
<td>Version 1 Host Timer</td>
<td>The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.</td>
</tr>
</tbody>
</table>

The following table is displayed to indicate all the sources associated with this group:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>The IP address of the source.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time elapsed in seconds since the source has been known.</td>
</tr>
</tbody>
</table>
**Layer 3 Routing Commands**

**Example**

```plaintext
console#show ipv6 mld groups ff1e::5

Interface..................................... vlan 6
Group Address................................ FF1E::5
Last Reporter................... FE80::200:FF:FE00:22
Up Time (hh:mm:ss).................... 00:03:43
Expiry Time (hh:mm:ss).............. ----
Filter Mode.................................. Include
Version1 Host Timer.................... ----
Group compat mode........................ v2

Source Address    ExpiryTime
-----------------  -----------
  4001::6         00:03:15
  4001::7         00:03:15
  4001::8         00:03:15

console#show ipv6 mld groups vlan 6

Group Address................................ FF1E::1
Interface..................................... vlan 6
Up Time (hh:mm:ss).................... 00:04:23
Expiry Time (hh:mm:ss).............. ----

Group Address................................ FF1E::2
Interface..................................... vlan 6
Up Time (hh:mm:ss).................... 00:04:23
Expiry Time (hh:mm:ss).............. ----

Group Address................................ FF1E::3
Interface..................................... vlan 6
Up Time (hh:mm:ss).................... 00:04:23
Expiry Time (hh:mm:ss).............. ----

Group Address................................ FF1E::4
Interface..................................... vlan 6
Up Time (hh:mm:ss).................... 00:04:23
Expiry Time (hh:mm:ss).............. ----
```

**show ipv6 mld interface**

The **show ipv6 mld interface** command is used to display MLD related information for an interface.
**Syntax**

show ipv6 mld interface { vlan vlan-id | all}

- vlan-id — A valid VLAN id.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following information is displayed for the specified interface:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number in unit/slot/port format.</td>
</tr>
<tr>
<td>MLD Global Admin Mode</td>
<td>This field displays the configured global administrative status of MLD.</td>
</tr>
<tr>
<td>MLD Interface Admin Mode</td>
<td>This field displays the configured interface administrative status of MLD.</td>
</tr>
<tr>
<td>MLD Operational Mode</td>
<td>The operational status of MLD on the interface.</td>
</tr>
<tr>
<td>MLD Version</td>
<td>This field indicates the version of MLD configured on the interface.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>This field indicates the configured query interval for the interface.</td>
</tr>
<tr>
<td>Query Max Response Time</td>
<td>This field indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.</td>
</tr>
<tr>
<td>Robustness</td>
<td>This field displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.</td>
</tr>
<tr>
<td>Startup Query Interval</td>
<td>This value indicates the configured interval between General Queries sent by a Querier on startup.</td>
</tr>
<tr>
<td>Startup Query Count</td>
<td>This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.</td>
</tr>
</tbody>
</table>
The following information is displayed if the operational mode of the MLD interface is enabled:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Member Query Interval</td>
<td>This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.</td>
</tr>
<tr>
<td>Last Member Query Count</td>
<td>This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.</td>
</tr>
</tbody>
</table>

The following information is displayed if the operational mode of the MLD interface is enabled:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier Status</td>
<td>This value indicates whether the interface is a MLD querier or non-querier on the subnet with which it is associated.</td>
</tr>
<tr>
<td>Querier Address</td>
<td>The IP address of the MLD querier on the subnet the interface with which it is associated.</td>
</tr>
<tr>
<td>Querier Up Time</td>
<td>Time elapsed in seconds since the querier state has been updated.</td>
</tr>
<tr>
<td>Querier Expiry Time</td>
<td>Time left in seconds before the Querier losses its title as querier.</td>
</tr>
<tr>
<td>Wrong Version Queries</td>
<td>Indicates the number of queries received whose MLD version does not match the MLD version of the interface.</td>
</tr>
<tr>
<td>Number of Joins</td>
<td>The number of times a group membership has been added on this interface.</td>
</tr>
<tr>
<td>Number of Leaves</td>
<td>The number of times a group membership has been removed on this interface.</td>
</tr>
<tr>
<td>Number of Groups</td>
<td>The current number of membership entries for this interface.</td>
</tr>
</tbody>
</table>

**Example**

console#show ipv6 mld interface vlan 2

```
Interface......................... vlan 2
MLD Global Admin Mode............ Enabled
MLD Interface Admin Mode........... Disabled
MLD Operational Mode.............. Disabled
MLD Version....................... 2
Query Interval (secs)............. 100
Query Max Response Time(milli-secs)........ 1111
Robustness.......................... 2
Startup Query Interval (secs)....... 31
```
show ipv6 mld host-proxy

Use the `show ipv6 mld host-proxy` command to display a summary of the host interface status parameters.

**Syntax**

`show ipv6 mld host-proxy`

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**Default Configuration**

There is no default configuration for this command.

**User Guidelines**

The command displays the following parameters only when you enable MLD Proxy:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The interface number of the MLD Proxy interface.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Indicates whether MLD Proxy is enabled or disabled. This is a configured value.</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>Indicates whether MLD Proxy is operationally enabled or disabled. This is a status parameter.</td>
</tr>
<tr>
<td>Version</td>
<td>The present MLD host version that is operational on the proxy interface.</td>
</tr>
<tr>
<td>Number of Multicast Groups</td>
<td>The number of multicast groups that are associated with the MLD-Proxy interface.</td>
</tr>
<tr>
<td>Unsolicited Report Interval</td>
<td>The time interval at which the MLD-Proxy interface sends unsolicited group membership reports.</td>
</tr>
</tbody>
</table>
Example

console#show ipv6 mld host-proxy
Interface Index................................... vlan 10
Admin Mode............................................ Enabled
Operational Mode................................. Enabled
Version.................................................. 3
Num of Multicast Groups........................... 0
Unsolicited Report Interval....................... 1
Querier IP Address on Proxy Interface........... fe80::1:2:5
Older Version 1 Querier Timeout............... 00:00:00
Proxy Start Frequency......................... 1

show ipv6 mld host-proxy groups

Use the show ipv6 mld host-proxy groups command to display information about multicast groups that the MLD Proxy reported.

Syntax

show ipv6 mld host-proxy groups

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

The following parameters are displayed by this command:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MLD Proxy interface.</td>
</tr>
</tbody>
</table>
Example

console#show ipv6 mld host-proxy groups
detailed information about multicast groups that MLD Proxy reported.

Syntax

show ipv6 mld host-proxy groups detail

Default Configuration

There is no default configuration for this command.
**Command Mode**
Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following parameters are displayed by this command:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number of the MLD-Proxy.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of the host that last sent a membership report for the current group on the network attached to the MLD Proxy interface (upstream interface).</td>
</tr>
<tr>
<td>Up Time (in secs)</td>
<td>The time elapsed in seconds since last created.</td>
</tr>
<tr>
<td>Member State</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Idle_Member—The interface has responded to the latest group membership query for this group.</td>
</tr>
<tr>
<td></td>
<td>• Delay_Member—The interface is going to send a group membership report to respond to a group membership query for this group.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>Possible values are Include or Exclude.</td>
</tr>
<tr>
<td>Sources</td>
<td>The number of sources attached to the multicast group.</td>
</tr>
<tr>
<td>Group Source List</td>
<td>The list of IP addresses of the sources attached to the multicast group.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time left for a source to get deleted.</td>
</tr>
</tbody>
</table>

**Example**

console#show ipv6 mld host-proxy groups
Interface................................ vlan 10

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Last Reporter</th>
<th>Up Time</th>
<th>Member State</th>
<th>Filter Mode</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF1E::1</td>
<td>FE80::100:2.3</td>
<td>244</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>2</td>
</tr>
</tbody>
</table>

Group Source List

Expiry Time
show ipv6 mld host-proxy interface

Use the `show ipv6 mld-proxy interface` command to display a detailed list of the host interface status parameters.

**Syntax**

```
show ipv6 mld host-proxy interface
```

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following parameters are displayed only when MLD Proxy is enabled:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MLD Proxy interface.</td>
</tr>
</tbody>
</table>

The column headings of the table associated with the interface are as follows:
Example

console#show ipv6 mld host-proxy interface

Interface................................ vlan 10

<table>
<thead>
<tr>
<th>Ver</th>
<th>Query Rcvd</th>
<th>Report Rcvd</th>
<th>Report Sent</th>
<th>Leaves Rcvd</th>
<th>Leaves Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>-----</td>
<td>-----</td>
</tr>
</tbody>
</table>

show ipv6 mld traffic

The `show ipv6 mld traffic` command is used to display MLD statistical information for the router.

Syntax

`show ipv6 mld traffic`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following fields are displayed:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid MLD Packets Received</td>
<td>The number of valid MLD packets received by the router.</td>
</tr>
<tr>
<td>Valid MLD Packets Sent</td>
<td>The number of valid MLD packets sent by the router.</td>
</tr>
<tr>
<td>Queries Received</td>
<td>The number of valid MLD queries received by the router.</td>
</tr>
<tr>
<td>Queries Sent</td>
<td>The number of valid MLD queries sent by the router.</td>
</tr>
<tr>
<td>Reports Received</td>
<td>The number of valid MLD reports received by the router.</td>
</tr>
<tr>
<td>Reports Sent</td>
<td>The number of valid MLD reports sent by the router.</td>
</tr>
<tr>
<td>Leaves Received</td>
<td>The number of valid MLD leaves received by the router.</td>
</tr>
<tr>
<td>Leaves Sent</td>
<td>The number of valid MLD leaves sent by the router.</td>
</tr>
<tr>
<td>Bad Checksum MLD Packets</td>
<td>The number of bad checksum MLD packets received by the router.</td>
</tr>
<tr>
<td>Malformed MLD Packets</td>
<td>The number of malformed MLD packets received by the router.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ipv6 mld traffic

Valid MLD Packets Received..................... 52
Valid MLD Packets Sent......................... 7
Queries Received............................... 0
Queries Sent................................... 7
Reports Received............................... 52
Reports Sent................................... 0
Leaves Received................................ 0
Leaves Sent.................................... 0
Bad Checksum MLD Packets...................... 0
Malformed MLD Packets.......................... 0
```

**show ipv6 nd raguard policy**

Use this command to display the RA Guard policy on all interfaces for which it is enabled.
Syntax
show ipv6 nd raguard policy

Default Configuration
By default, no RA guard policies are applied to any interface.

Command Mode
Privileged Exec, Global Configuration

User Guidelines
This command has no user guidelines.

Command History
Introduced in version 6.2.0.1 firmware.

Example
The following example configures an unnamed RA Guard policy to drop all RA advertisements and router redirect messages on interface Gi1/0/1 (VLAN 10). The configured interfaces are shown.

```
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface vlan 10
console(config-if-vlan10)#ipv6 enable
console(config-if-vlan10)#exit
console(config)#ipv6 unicast-routing
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport access vlan 10
console(config-if-Gi1/0/1)#exit
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#ipv6 nd raguard attach-policy
console(config-if-Gi1/0/1)#show ipv6 nd raguard policy
```

<table>
<thead>
<tr>
<th>Ipv6 RA-Guard Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>
show ipv6 neighbors

Use the show ipv6 neighbors command to display information about the IPv6 neighbors.

Syntax

show ipv6 neighbors

Default Configuration

This command has no default configuration.

Command Mode

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the IPv6 neighbors.

```
console(config)#show ipv6 neighbors
Neighbor Last IPv6 Address         MAC Address       isRtr  State   Updated
                   Interface
-------------------- ----------------- -----  ------- ---------
```

show ipv6 protocols

Use the show ipv6 protocols command to display information about the configured IPv6 routing protocols

Syntax

show ipv6 protocols

Default Configuration

There is no default configuration for this command.
**Command Mode**
Privileged Exec mode, Global Configuration mode, all Configuration submodes.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console#show ipv6 protocols
Routing Protocol ......................... BGP
BGP Router ID ............................ 255.255.255.255
Local AS Number .......................... 1
BGP Admin Mode ............................ Enable
Maximum Paths ............................. Internal 3, External 2
Always compare MED ........................ TRUE
Maximum AS Path Length ................... 100
Fast Internal Failover .................... Disable
Fast External Failover .................... Disable
Distance .................................. Ext 126, Int 127, Local 126

Prefix List In ............................ none
Prefix List Out ........................... none

Redistributing:
Source    Metric     Dist List                        Route Map
--------- ---------- -------------------------------- ----------------------
----------
connected

Networks Originated:

Neighbors:
2001::1
  Filter List In ........................ 1
  Filter List Out ....................... 1

Routing Protocol ........................ OSPFv3
Router ID ................................. 0.0.0.0
OSPF Admin Mode .......................... Disable
Maximum Paths ............................ 4
Routing for networks ..................... Not Configured
Distance .................................. Intra 110 Inter 110 Ext 110
Default Route Advertise .................. Disabled
Always ..................................... False
Metric ..................................... Not configured
Metric Type ............................... External Type 2
```
show ipv6 route

Use the show ipv6 route command in User Exec or Privileged Exec mode to display the IPv6 routing table. The output of the command also displays the IPv6 address of the default gateway and the default route associated with the gateway.

Syntax

show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface-type interface-number] [best]

- **ipv6-address**—Specifies an IPv6 address for which the best-matching route would be displayed.
- **protocol**—Specifies the protocol that installed the routes. Is one of the following keywords: connected, ospf, static.
- **ipv6-prefix/ prefix-length**— Specifies an IPv6 network for which the matching route would be displayed.
- **interface-type interface-number**—Valid IPv6 interface. Specifies that the routes with next-hops on the selected interface be displayed. Supported interface types are VLAN, Tunnel, and Loopback.
- **best**—Specifies that only the best routes are displayed. If the connected keyword is selected for protocol, the best option is not available because there are no best or non-best connected routes.

Default Configuration

This command has no default configuration.

Command Mode

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.
Example
The following example displays the IPv6 address of the default gateway and the default route associated with the gateway.

```
console(config)#show ipv6 route
IPv6 Routing Table - 0 entries
Route Codes: C - connected, S - static
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
Default gateway is 10.1.20.1
S  0.0.0.0/0 [254/0] via 10.1.20.1
C  10.1.20.0/24 [0/1] directly connected, vlan2
C  20.1.20.0/24 [0/1] directly connected, vlan4
```

**show ipv6 route preferences**

Use the `show ipv6 route preferences` command to show the preference value associated with the type of route. Lower numbers have a greater preference.

**Syntax**

```
show ipv6 route preferences
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example shows the preference value associated with the type of route.

```
console#show ipv6 route preferences
Local.......................... 0
```
show ipv6 route summary

Use the `show ipv6 route summary` command to display a summary of the routing table for all routes, including best and non-best routes. Use `best` to display the count summary for only best routes.

**Syntax**

```
show ipv6 route summary [best]
```

- `best` — Displays the count summary for only best routes.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Command History**

Updated in version 6.3.0.1 firmware.

**Example**

The following example displays a summary of the routing table.

```
console#show ipv6 route summary

Connected Routes...............................32
Static Routes.................................. 0
6To4 Routes.................................... 0
BGP Routes..................................... 10
```
show ipv6 snooping counters
Use this command to display the RA guard dropped packet counters.

Syntax
show ipv6 snooping counters [interface interface-id ]
  • interface-id—An interface identifier (Ethernet or port-channel).

Default Configuration
By default, no RA guard policies are applied to any interface.

Command Mode
Privileged Exec, Global Configuration, and all submodes

User Guideline
There are no user guidelines for this command.

Command History
Introduced in version 6.2.0.1 firmware.

Example
console(config-if-vlan10)#show ipv6 snooping counters

IPv6 Dropped Messages

<table>
<thead>
<tr>
<th>Interface</th>
<th>RA</th>
<th>REDIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show ipv6 traffic

Use the show ipv6 traffic command in User Exec mode to show traffic and statistics for IPv6 and ICMPv6.

Syntax

show ipv6 traffic [vlan vlan-id | tunnel tunnel-id | loopback loopback-id]

- vlan-id — Valid VLAN ID, shows information about traffic on a specific interface or, without the optional parameter, shows information about traffic on all interfaces.
- tunnel-id — Tunnel identifier. (Range: 0-7)
- loopback-id — Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Examples

The following examples show traffic and statistics for IPv6 and ICMPv6, first for all interfaces and an individual VLAN.

console> show ipv6 traffic
IPv6 STATISTICS
Total Datagrams Received................................. 0
Received Datagrams Locally
Delivered....................................................... 0
Received Datagrams Discarded Due To Header Errors.. 0
Received Datagrams Discarded Due To MTU............. 0
Received Datagrams Discarded Due To No Route....... 0
Received Datagrams With Unknown Protocol............ 0
Received Datagrams Discarded Due To Invalid Address.0
console> show ipv6 traffic vlan 11
Interface .............................. 11
IPv6 STATISTICS
Total Datagrams Received.............. 0
Received Datagrams Locally Delivered 0
Received Datagrams Discarded Due To Header Errors 0
Received Datagrams Discarded Due To MTU........ 0
Red Datagrams Discarded Due To No Route........ 0
Received Datagrams With Unknown Protocol........ 0
Received Datagrams Discarded Due To Invalid Address 0
Received Datagrams Discarded Due To Truncated Data 0
Received Datagrams Discarded Other......... 0
Received Datagrams Reassembly Required..... 0
Datagrams Successfully Reassembled....... 0
Datagrams Failed To Reassemble........... 0
Datagrams Forwarded........................ 0
Datagrams Locally Transmitted........... 0
Datagrams Transmit Failed.............. 0
Datagrams Successfully Fragmented....... 0
Datagrams Failed To Fragment............... 0
Fragments Created........................ 0
Multicast Datagrams Received............ 0
Multicast Datagrams Transmitted.......... 0

show ipv6 vlan
Use the show ipv6 vlan command to display IPv6 VLAN routing interface addresses.

Syntax
show ipv6 vlan
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays IPv6 VLAN routing interface addresses.

```
console#show ipv6 vlan
MAC Address used by Routing VLANs: 00:02:BC:00:30:68
VLAN ID  IPv6 Address/Prefix Length
-------  ---------------------------------------
1
```

traceroute ipv6
Use the traceroute ipv6 command to determine the path and measure the transit delay to another device in the network. The transit delays are measured for each hop in the network.

Syntax
```
traceroute ipv6 {ipv6-address | hostname} [count 1-10] [init-ttl 1-255] [interval 1-60] [max-fail 0-255] [max-ttl 1-255] [port 1-65535] [size 0-39936] [source {ipv6-address | loopback loopback-id | vlan vlan-id}]
```

- ipv6-address | hostname—The target IP address or host to ping.
- out-of-band—Send the ping over the out-of-band interface.
- vlan-id—The VLAN over which to send the echo request.
- loopback-id—Use the source address from the selected loopback. (Range 0-7)
- count—The number of echo request packets to send for each ttl value. (Range 1-10. Default 3).
Layer 3 Routing Commands

- interval—The time (in seconds) between successive echo requests. Default 3.
- init-ttl—The initial TTL sent in the ICMP echo request packets (Range 1-255. Default 1).
- max-ttl—The maximum ttl sent in the ICMP echo request packet (Range 1-255, default 30). Must be equal to or larger than init-ttl.
- port—The destination UDP port of the probe. (Range 1-65535).
- size—The packet size padding in bytes. (Range 0-39936, default 0).
- source—Use the specified source IP address, loopback address, VLAN address, tunnel or out-of-band interface address in the transmitted packets.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec and User Exec modes

User Guidelines
Traceroute operates by sending a sequence of Internet Control Message Protocol (ICMP) echo request packets. The time-to-live (TTL) value, is used in determining the intermediate routers through which the packet flows toward the destination address. Routers decrement a packet’s TTL value and discard packets whose TTL equals 0. On discarding a packet, the router returns an ICMP time exceeded message to the source.

Example
(console)# traceroute ipv6 2001::2 init-ttl 1 max-ttl 4 max-fail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2, 4 hops max, 43 byte packets:
1 2001::2 708 msec 41 msec 11 msec
2 2001::2 12 msec 13 msec 12 msec
3 2001::2 14 msec 9 msec 11 msec
Loopback Interface Commands

Dell EMC Networking N1500/N2000/N3000/N3100/N4000 Series Switches

Dell EMC Networking provides for the creation, deletion, and management of loopback interfaces. They are dynamic interfaces that are created and deleted by user configuration.

A loopback interface is always expected to be up. As such, it provides a means to configure a stable IP address on the device which may be referred to by other switches in the network. This interface never transmits data but may receive data. It is typically expected to be used by routing protocols.

Loopback interfaces will respond to pings.

Loopback interfaces are not supported on the N1100-ON Series switches.

Commands in this Section

This section explains the following commands:

```
interface loopback                  show interfaces loopback
```

**interface loopback**

Use the `interface loopback` command in Global Configuration mode to enter the Interface Loopback configuration mode.

**Syntax**

```
interface loopback loopback-id
no interface loopback loopback-id
```

- loopback-id — Loopback identifier. (Range: 0-7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode.
**User Guidelines**

This command has no user guidelines.

**Example**

The following example enters the Interface Loopback 1 configuration mode.

```plaintext
console(config)#interface loopback 1
console(config-if-loopback0)#ip address 192.168.22.1 255.255.255.255
console(config-if-loopback0)#exit
console(config)#ex
console#ping 192.168.22.1
  Pinging 192.168.22.1 with 0 bytes of data:

  Reply From 192.168.22.1: icmp_seq = 0. time <10 msec.
  Reply From 192.168.22.1: icmp_seq = 1. time <10 msec.
  Reply From 192.168.22.1: icmp_seq = 2. time <10 msec.
  Reply From 192.168.22.1: icmp_seq = 3. time <10 msec.
```

**show interfaces loopback**

Use the `show interfaces loopback` command to display information about one or all configured loopback interfaces.

**Syntax**

```
show interfaces loopback [loopback-id]
```

- `loopback-id` — Loopback identifier. (Range: 0-7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Loopback interfaces are not supported on the N1100-ON Series switches.
Examples

The following examples display information about configured loopback interfaces.

```
console# show interfaces loopback
Loopback Id Interface IP Address Received Packets Sent Packets
---------- --------- ---------- ---------------- ------------
1          loopback 1 0.0.0.0   0                 0

console# show interfaces loopback 1
Interface Link Status.......................... Up
IP Address..................................... 0.0.0.0 0.0.0.0
MTU size....................................... 1500 bytes
```
IP Multicast Commands

The Dell Network N1500/N2000/N2100-ON series supports limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

The Dell EMC Networking multicast component is best suited for video and audio traffic requiring multicast packet control for optimal operation. The multicast component includes support for IGMPv2, IGMPv3, PIM-DM, PIM-SM, and DVMRP. Communication from point to multipoint is called multicasting. The source host (point) transmits a message to a group of zero or more hosts (multipoint) that are identified by a single IP destination address. Although the task may be accomplished by sending unicast (point-to-point) messages to each of the destination hosts, multicasting is the more desirable method for this type of transmission. A multicast message is delivered to all members of its destination host group with the same best-efforts reliability as regular unicast IP messages. The message is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other messages. The advantages of multicasting are explained below:

- **Network Load Decrease:** A number of applications are required to transmit packets to hundreds of stations. The packets transmitted to these stations share a group of links on their paths to their destinations. Multicast transmission can conserve much needed network bandwidth, since multicasting transmission requires the transmission of only a single packet by the source and replicates this packet only if it is necessary (at forks of the multicast delivery tree).

- **Discovery of resources:** A number of applications require a host to find out whether a certain type of service is available. Internet protocols such as Bootstrap Protocol (BOOTP) and Open Shortest Path First (OSPF) protocol are among these applications. Using multicast messages and sending the query to those hosts which are potentially capable of providing this service speeds the gathering of this information considerably. Although a group of hosts residing on the same network are the intended target for the majority of multicast packets, this limitation is not
mandatory. Discovering the local domain-name server is the intended use of multicast messages on remote networks when there is less than one server per network.

- Applications used for datacasting: Since multimedia transmission has become increasingly popular, multicast transmission use has increased. Multicast transmission may be used to efficiently accommodate this type of communication. For instance, the audio and video signals are captured, compressed and transmitted to a group of receiving stations. Instead of using a set of point-to-point connections between the participating nodes, multicasting can be used for distribution of the multimedia data to the receivers. The participating stations are free to join or leave an audio-cast or a video-cast as needed. The variable membership maintenance is managed efficiently through multicasting.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear ip mroute</th>
<th>ip pim dense-mode</th>
<th>show ip mfc</th>
<th>show ip mroute static</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>ip pim dr-priority</td>
<td>show ip multicast</td>
<td>show ip pim</td>
</tr>
<tr>
<td>ip mroute</td>
<td>ip pim hello-interval</td>
<td>show ip pim</td>
<td>show ip mroute interface</td>
</tr>
<tr>
<td>ip multicast-routing</td>
<td>ip pim join-prune-interval</td>
<td>show ip multicast interface</td>
<td>show ip pim interface</td>
</tr>
<tr>
<td>ip multicast ttl-threshold</td>
<td>ip pim rp-address</td>
<td>show ip mroute</td>
<td>show ip pim neighbor</td>
</tr>
<tr>
<td>ip pim</td>
<td>ip pim rp-candidate</td>
<td>show ip mroute</td>
<td>show ip pim rp-hash</td>
</tr>
<tr>
<td>ip pim bsr-border</td>
<td>ip pim sparse-mode</td>
<td>show ip mroute</td>
<td>show ip pim rp mapping</td>
</tr>
<tr>
<td>ip pim bsr-candidate</td>
<td>ip pim ssm</td>
<td>–</td>
<td>show ip pim statistics</td>
</tr>
</tbody>
</table>

**clear ip mroute**

Use this command to selectively clear IPv4 multicast entries from the cache.
**Syntax**

```
clear ip mroute { * | group-address [ source-address ] }
```
- * —Deletes all IPv4 entries from the IP multicast routing table.
- group-address — IP address of the multicast group.
- source-address — IP address of a multicast source that is sending multicast traffic to the group.

**Default configuration**

There is no default configuration for this command.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

When a * entry is deleted through this command, it cannot be formed again until it is expired in IGMP and started again via the host. The default mcache time-out is 210 seconds.

**Example**

The following example deletes all entries from the IP multicast routing table:

```
console# clear ip mroute *
```

The following example deletes from the IP multicast routing table all entries that match the given multicast group address (239.1.2.1), irrespective of which source is sending for this group:

```
console# clear ip mroute 239.1.2.1
```

The following example deletes from the IP multicast routing table all entries that match the given multicast group address (239.1.2.1) and the multicast source address (192.168.10.10):

```
console# clear ip mroute 239.1.2.1 192.168.10.10
```
**ip multicast boundary**

Use the `ip multicast boundary` command in Interface Configuration mode to add an administrative scope multicast boundary specified by `groupipaddr` and `mask` for which this multicast administrative boundary is applicable. `groupipaddr` is a group IP address and `mask` is a group IP mask.

**Syntax**

```
ip multicast boundary groupipaddr mask
no ip multicast boundary groupipaddr
```

- `groupipaddr` — IP address of multicast group. Valid range is 239.0.0.0 to 239.255.255.255.
- `mask` — The group address mask in dotted quad notation.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

The administratively scoped multicast address range is 239.0.0.0 to 239.255.255.255

**Example**

The following example adds an administrative scope multicast boundary.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip multicast boundary 239.5.5.5 255.255.255.255
```

**ip mrout**

Use the `ip mroute` command to create a static multicast route for a source range. Use the `no` form of this command to delete a static multicast route.

**Syntax**

```
ip mroute source-address mask rpf-address preference
```

no ip mroute source-address mask

- source-address — The IP address of the multicast data source.
- mask — The IP subnet mask of the multicast data source.
- rpf-address — The IP address of the next hop towards the source.
- preference — The cost of the route (Range: 1 - 255).

Default Configuration
There is no default configuration for this command.

Command Mode
Global Configuration mode

User Guidelines
The source IP address must contain 0's for the address bits corresponding the 0's in the netmask.

Multicast source data is flooded/forwarded by default in the VLAN on which it is received. For this reason, multi-access VLANs are not recommended for multicast routing interfaces.

Example
console(config)#ip mroute 1.1.0.0 255.255.0.0 192.168.20.1 34

ip multicast-routing
Use the ip multicast-routing command in Global Configuration mode to set the administrative mode of the IP multicast forwarder in the router to active. It enables both IPv4 and IPv6 multicast routing. For multicast routing to become operational, IGMP must be currently enabled. Enabling PIM or DVMRP enables IGMP.

Syntax
ip multicast-routing
no ip multicast-routing
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
Use of a multicast routing protocol is recommended (e.g., PIM) when IP multicast is enabled.
IGMP/MLD snooping may be enabled when IP multicast is enabled. If a multicast source is connected to a VLAN on which both L3 multicast and IGMP/MLD snooping are enabled, the multicast source is forwarded to the mrouter ports that have been discovered when the multicast source is first seen. If a new mrouter is later discovered on a different port, the multicast source data is not forwarded to the new port. Likewise, if an existing mrouter times out or stops querying, the multicast source data continues to be forwarded to that port. If a host in the VLAN subsequently joins or leaves the group, the list of mrouter ports is updated for the multicast source and the forwarding of the multicast source is adjusted. The workaround to this limitation is to statically configure mrouter ports when enabling IGMP/MLD snooping in L3 multicast enabled VLANs.
Multicast routing requires IGMP to be enabled to become operationally enabled. Enabling PIM or DVMRP enables IGMP.
This command enables both IPv4 and IPv6 multicast routing. Multicast source data is flooded/forwarded by default in the VLAN on which it is received. For this reason, multi-access VLANs are not recommended for multicast routing interfaces.

Example
The following example enables IP multicast on the router.

```
console#configure
cconsole(config)#ip multicast-routing
```

Command History
**ip multicast ttl-threshold**

Use the `ip multicast ttl-threshold` command in Interface VLAN Configuration mode to apply a `ttlvalue` to a routing interface. `ttlvalue` is the TTL threshold which is applied to the multicast Data packets forwarded through the interface.

**Syntax**

```
ip multicast ttl-threshold ttlvalue
no ip multicast ttl-threshold
```

- `ttlvalue` — Specifies TTL threshold. (Range: 0-255)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example applies a `ttlvalue` of 5 to the VLAN 15 routing interface.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip multicast ttl-threshold 5
```

**ip pim**

Use the `ip pim` command in Interface (VLAN) Configuration mode to administratively configure PIM mode for IP multicast routing on a VLAN interface. Enabling or disabling PIM mode concurrently enables/disables IGMP. Use the `no` form of the command to disable PIM on the interface.

**Syntax**

```
ip pim
```

no ip pim

**Default Configuration**
PIM is not enabled on interfaces by default.

**Command Mode**
Interface (VLAN) Configuration mode

**User Guidelines**
PIM requires that routing and multicast routing be enabled. Enabling PIM enables IGMP/MLD. Disabling PIM may operationally disable multicast routing.

**Example**
```
console(config)#ip routing
console(config)#ip multicast
console(config)#interface vlan 10
console(if-vlan-10)#ip pim
```

**Command History**
User Guidelines updated in release 6.3.5.

**ip pim bsr-border**
The `ip pim bsr-border` command is used in Interface (VLAN) Configuration mode to administratively disable bootstrap router (BSR) messages on the interface. Use the `no` form of this command to return the configuration to the default.

**Syntax**
```
ip pim bsr-border
no ip pim bsr-border
```

**Default Configuration**
BSR messages are enabled on the interface by default.
**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

This command only has an effect if sparse mode is enabled.

**Example**

```console
console(if-vlan-10)#ip pim bsr-border
```

**ip pim bsr-candidate**

The `ip pim bsr-candidate` command is used to configure the router to advertise itself as a bootstrap router (BSR). Use the `no` form of this command to return to the default configuration. This command replaces the `ip pimsm bsr-candidate`, `ip pimsm cbsrhaskmasklength` and `ip pimsm cbsrpvalue` commands.

**Syntax**

```plaintext
ip pim bsr-candidate vlan {vlan-id hash-mask-length bsr-priority [interval interval]}
no ip pim bsr-candidate vlan {vlan-id}
```

- `vlan-id`—A valid VLAN identifier with multicast routing enabled.
- `hash-mask-length` —Length of the BSR hash to be ANDed with the multicast group address. (Range 0–32 bits). Default 0.
- `bsr-priority`—The advertised priority of the BSR candidate. Range 0-255. Default 0.
- `interval`—(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

**Default Configuration**

None - the router does not advertise itself as a BSR candidate.

**Command Mode**

Global Configuration mode
User Guidelines

All multicast groups with the same hash value correspond to the same RP. Lower priority values are preferred.

Example

```
console(config)#ip pim bsr-candidate vlan 10 16 0 interval 30
```

ip pim dense-mode

Use the `ip pim dense-mode` command in Global Configuration mode to administratively configure PIM dense mode for IP multicast routing. Use the `no` form of this command to disable PIM.

Syntax

```
ip pim dense-mode
no ip pim
```

Default Configuration

PIM is not enabled by default.

Command Mode

Global Configuration mode

User Guidelines

Only one of sparse or dense mode can be configured on a router. IGMP is automatically enabled if PIM is enabled and disabled when PIM is disabled. `ip multicast-routing` may be operationally enabled or disabled by this command.

PIM is not compatible with DVMRP. DVMRP must be disabled before enabling PIM.

Example

```
console(config)#ip multicast-routing
console(config)#ip pim dense-mode
```
**ip pim dr-priority**

The `ip pim dr-priority` command in Interface (VLAN) Configuration mode to administratively configure the advertised designated router (DR) priority value. Use the `no` form of this command to return the configuration to the default.

**Syntax**

```
ip pim dr-priority priority
no ip pim dr-priority
```

- `priority` — The administratively configured priority (Range: 0–2147483647).

**Default Configuration**

The default election priority is 1.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

This command only has an effect if sparse mode is enabled. Lower values are preferred.

**Example**

```
console(if-vlan10)#ip pim dr-priority 32768
```

**ip pim hello-interval**

The `ip pim hello-interval` command in Interface (VLAN) Configuration mode to administratively configure the frequency of PIM Hello messages on the specified interface. Use the `no` form of this command to return the configuration to the default.

**Syntax**

```
ip pim hello-interval interval
no ip pim hello-interval
```
• interval — The number of seconds between successive hello transmissions. Range: 0–18000 seconds. Default is 30.

**Default Configuration**
The default hello interval is 30 seconds.

**Command Mode**
Interface (VLAN) Configuration mode

**User Guidelines**
There are no user guidelines for this command.

**Example**

```bash
console(config-if-vlan10)#ip pim hello-interval 20
```

**ip pim join-prune-interval**
The `ip pim join-prune-interval` command in Interface (VLAN) Configuration mode to administratively configure the frequency of join/prune messages on the specified interface. Use the `no` form of this command to return the configuration to the default.

**Syntax**

```
ip pim join-prune-interval interval
no ip pim join-prune-interval
```

• interval — The number of seconds between successive join-prune transmissions. Range: 0–18000 seconds. Default is 60.

**Default Configuration**
The default join/prune interval is 60 seconds.

**Command Mode**
Interface (VLAN) Configuration mode
User Guidelines

This command only has an effect if sparse mode is enabled.

Example

console(if-vlan10)#ip pim join-prune-interval 30

ip pim rp-address

Use the `ip pim rp-address` command in Global Configuration mode to define the address of a PIM Rendezvous point (RP) for a specific multicast group range. Use the `no` form of this command to remove a configured RP. This command replaces the `ip pimsm rp-address` command.

Syntax

```
ip pim rp-address {rp-address group-address group-mask [override]}
no ip pim rp-address {rp-address group-address group-mask}
```

- `rp-address` — The valid IPv4 address for the rendezvous point.
- `group-address` — A valid multicast group address to be sourced from the rendezvous point.
- `group-mask` — A mask indicating the range of multicast groups sourced from the RP.
- `override` — A flag indicating that the static entry should override dynamically learned entries for the configured multicast group.

Default Configuration

None — no static multicast groups are configured for an RP.

Command Mode

Global Configuration mode

User Guidelines

A maximum of 32 multicast group ranges may be defined for each rendezvous point. The configured ranges may not overlap.
Command History
Updated guidelines in version 6.5 firmware.

Example
console(config)#ip pim rp-address 192.168.21.1 239.1.0.0 255.255.0.0 override

ip pim rp-candidate

Use the ip pim rp-candidate command in Global Configuration mode to configure the router to advertise itself to the bootstrap router (BSR) router as a PIM candidate rendezvous point (RP) for a specific multicast group range. Use the no form of this command to return to the default configuration. This command replaces the ip pimsrn rp-candidate command.

Syntax
ip pim rp-candidate vlan {vlan-id group-address group-mask [interval interval]}
no ip pim rp-candidate vlan vlan-id group-address group-mask}

• vlan-id—A valid VLAN identifier with multicast routing enabled.
• group-address—A valid multicast group address.
• group-mask—A mask indicating the range of multicast groups for which the router should advertise itself as an RP-candidate.
• interval—(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default Configuration
None - the router does not advertise itself as an RP candidate by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.
**ip pim sparse-mode**

Use the **ip pim sparse-mode** command in Global Configuration mode to administratively configure PIM sparse mode for IP multicast routing. Use the **no** form of this command to disable PIM.

**Syntax**

```
ip pim sparse-mode
no ip pim
```

**Default Configuration**

PIM not enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Only one of sparse or dense mode can be configured on a router. IGMP is automatically enabled if PIM is enabled and disabled when PIM is disabled. IP multicast must be enabled for PIM to operate. **ip multicast-routing** is not disabled or enabled by this command.

It is recommended that IGMP snooping be disabled if IP multicast is enabled unless specifically required. PIM is not compatible with DVMRP. DVMRP must be disabled before enabling PIM.

**Example**

```
console(config)#ip pim sparse-mode
```
**ip pim ssm**

Use the `ip pim ssm` command in Global Configuration mode to administratively configure PIM source specific multicast range of addresses for IP multicast routing. Use the `no` form of this command to remove configured ranges of addresses from the router.

**Syntax**

```
ip pim ssm {default | group-address group-mask}
no ip pim ssm {default | group-address group-mask}
```

- **default**—Defines the SSM range access list to 232/8.
- **group-address**—An IP multicast group address.
- **group-mask**—An IPv4 mask in a.b.c.d form where a, b, c and d range from 0-255.

**Default Configuration**

There are no group addresses configured by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config)#ip pim ssm 239.0.10.0 255.255.255.0
```

**show ip mfc**

Use the `show ip mfc` command to display the multicast forwarding cache.

**Syntax**

```
show ip mfc
```
Default Configuration
This command does not have a default configuration.

Command Mode
Privileged Exec mode, Global Config mode, all sub-modes.

User Guidelines
This command display both the IPv4 and IPv6 MFC entries.
The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFC IPv4 Mode</td>
<td>Enabled when IPv4 multicast routing is operational.</td>
</tr>
<tr>
<td>MFC IPv6 Mode</td>
<td>Enabled when IPv6 multicast routing is operational.</td>
</tr>
<tr>
<td>MFC Entry Count</td>
<td>The number of entries present in MFC.</td>
</tr>
<tr>
<td>Total Pkts Forwarded in SW</td>
<td>Total Number of multicast packets forwarded in software.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address of the multicast route entry.</td>
</tr>
<tr>
<td>Group Address</td>
<td>Group address of the multicast route entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The current operating multicast routing protocol.</td>
</tr>
<tr>
<td>Pkts Forwarded in SW</td>
<td>Number of multicast packets that are forwarded in software for a specific multicast route entry.</td>
</tr>
</tbody>
</table>

Example
```
console#show ip mfc
MFC IPv4 Mode................................. Disabled
MFC IPv6 Mode................................. Disabled
MFC Entry Count............................... 0
Current multicast IPv4 protocol............ PIMSM
Current multicast IPv6 protocol............ No protocol enabled.
Total software forwarded packets......... 0

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Group Address</th>
<th>Protocol</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.28.4</td>
<td>232.1.2.3</td>
<td>PIM-SM</td>
<td>61</td>
</tr>
</tbody>
</table>
```
**show ip multicast**

Use the `show ip multicast` command to display the system-wide multicast information.

**Syntax**

`show ip multicast`

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays system-wide multicast information.

```console
console#show ip multicast
Admin Mode...........................  Enabled
Protocol State.......................  Non-Operational
Table Max Size.......................  768
Protocol.............................  PIMDM
Multicast forwarding cache entry count 0
```

**show ip pim boundary**

Use the `show ip pim boundary` command to display all the configured administrative scoped multicast boundaries.

**Syntax**

`show ip pim boundary {vlan vlan-id | all}`

- `vlan-id` — Valid VLAN ID.
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays all the configured administrative scoped multicast boundaries.

```
console#show ip pim boundary all
MULTICAST BOUNDARY
Interface Group IP Mask
-------- ------ ---------------
```

show ip multicast interface
Use the `show ip multicast interface` command to display the multicast information for the specified interface.

Syntax
```
show ip multicast interface [type number]
```
- **type number**—Interface type and number for which to display IP multicast information. VLAN Vlan-ID is the only supported type and number.

Default Configuration
Show information for all multicast interfaces.

Command Mode
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes
**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the multicast information for VLAN 15.

```
console#show ip mcast interface vlan 15
Interface  TTL
----------  -----
Vl15        1
```

**show ip mroute**
Use the `show ip mroute` command to display a summary or details of the multicast table.

**Syntax**
```
show ip mroute
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
```
console#show ip mroute

IP Multicast route table
Source IP    Group IP    Expiry     Up Time    RPF Neighbor    Flags
-----------  ----------  --------    -------    ---------------    -----
192.168.0.11  239.0.5.7   3:03      15:54:12  192.168.0.10
```

Layer 3 Routing Commands | 1630
show ip mroute group

Use the **show ip mroute group** command to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the groupipaddr value.

**Syntax**

```
show ip mroute group groupipaddr [summary]
```

- `groupipaddr` — IP address of the multicast group.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces.

```
console#show ip mroute group 239.5.5.5 summary
console#show ip mroute group 239.5.5.5
```

**show ip mroute source**

Use the **show ip mroute source** command to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the sourceipaddr or sourceipaddr | groupipaddr pair value(s).
**Syntax**

```
show ip mroute source sourceipaddr {summary}
```

- `sourceipaddr` — IP address of source.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Use the summary option to summarize the information displayed.

**Example**

The following example displays multicast configuration settings.

```
console#show ip mroute source 10.1.1.1 summary
```

```
console#show ip mroute source 10.1.1.1 239.5.5.5
```

**show ip mroute static**

Use the `show ip mroute static` command to display all the static routes configured in the static mcast table if it is specified or display the static route associated with the particular sourceipaddr.

**Syntax**

```
show ip mroute static [sourceipaddr]
```

- `sourceipaddr` — IP address of source.

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the static routes configured in the static mcast table.

```
console#show ip mroute static
```

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source Mask</th>
<th>RPF Address</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>255.255.255.0</td>
<td>2.2.2.2</td>
<td>23</td>
</tr>
</tbody>
</table>

**show ip pim**
The `show ip pim` command displays information about the interfaces enabled for PIM.

**Syntax**

```
show ip pim
```

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following information is displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

Example

console#show ip pim

PIM Mode............................. None

If no routers are enabled for PIM, the following message is displayed.

None of the routing interfaces are enabled for PIM.

show ip pim bsr-router

The show ip pim bsr-router command displays information about a bootstrap router (BSR).

Syntax

show ip pim bsr-router {candidate|elected}

- candidate – Shows the candidate routers capable of acting as the bootstrap router.
- elected – Shows the router elected as the PIM bootstrap router.

Default Configuration

There is no default configuration for this command.

Command Mode

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following information is displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSR address</td>
<td>IP address of the BSR.</td>
</tr>
<tr>
<td>BSR Priority</td>
<td>The configured BSR priority.</td>
</tr>
<tr>
<td>BSR Hash Mask Length</td>
<td>The configured hash mask length (32 bits maximum).</td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

Example

console#show ip pim bsr-router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Bootstrap Message in</td>
<td>Time remaining (in hours, minutes, and seconds) until a BSR message is sent.</td>
</tr>
<tr>
<td>Next Candidate RP Advertisement</td>
<td>Time remaining (in hours, minutes, and seconds) until the next RP advertisement is sent.</td>
</tr>
</tbody>
</table>

If no configured/elected BSRs exist on the router, the following message is displayed.

No BSR’s exist/learned on this router.

**show ip pim interface**

The `show ip pim interface` command displays the PIM interface status parameters. If the interface number is not specified, the command displays the status parameters of all the PIM-enabled interfaces.

**Syntax**

`show ip pim interface [vlan vlan-id]`

- `vlan-id` — A valid VLAN ID for which multicast routing has been enabled.

**Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Active PIM Protocol</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Hello interval value</td>
</tr>
<tr>
<td>Join-prune Interval</td>
<td>Join-prune interval value</td>
</tr>
<tr>
<td>DR Priority</td>
<td>DR Priority configured on this interface</td>
</tr>
<tr>
<td>BSR Border</td>
<td>Whether or not this interface is configured as a BSR Border</td>
</tr>
</tbody>
</table>
Default Configuration
There is no default configuration for this command.

Command Mode
User Exec and Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.

Example
(console)#show ip pim interface

Interface VLAN0010
  Mode Sparse
  Hello Interval(secs) 30
  Join Prune Interval(secs) 60
  DR Priority 1
  BSR Border Disabled
  Neighbor Count 1
  Designated Router 192.168.10.1

Interface VLAN0001
  Mode Sparse
  Hello Interval(secs) 30
  Join Prune Interval(secs) 60
  DR Priority 1
  BSR Border Disabled
  Neighbor Count 1
  Designated Router 192.168.10.1

If none of the interfaces are enabled for PIM, the following message is displayed:

None of the routing interfaces are enabled for PIM

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Count</td>
<td>Number of PIM Neighbors learned on this interface</td>
</tr>
<tr>
<td>Designated-Router</td>
<td>IP address of the elected DR on the interface</td>
</tr>
</tbody>
</table>
show ip pim neighbor

Use the show ip pim neighbor command in User Exec or Privileged Exec modes to display PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM-enabled interfaces.

Syntax

show ip pim neighbor [vlan vlan-id]

- vlan-id — A valid VLAN ID for which multicast routing has been enabled.

Default Configuration

This command has no default configuration.

Command Mode

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines

The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Addr</td>
<td>IP address of the PIM neighbor</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time since the neighbor is learned</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time remaining for the neighbor to expire</td>
</tr>
</tbody>
</table>

Example

(console)#show ip pim neighbor vlan 10

Neighbor Addr | Interface | Up Time | Expiry Time
--------------|-----------|---------|---------------
192.168.10.2  | VLAN0010  | 00:02:55| 00:01:15

(console)#show ip pim neighbor

Neighbor Addr | Interface | Uptime   | Expiry Time
--------------|-----------|----------|---------------
               |           | (HH:MM:SS)| (HH:MM:SS)    |
If no neighbors are learned on any of the interfaces, the following message is displayed.

No neighbors are learned on any interface.

**show ip pim rp-hash**

The `show ip pim rp-hash` command displays the rendezvous point (RP) selected for the specified group address.

**Syntax**

```
show ip pim rp-hash group-address
```

- `group-address` — A valid multicast address supported by RP.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>Address of the RP</td>
</tr>
<tr>
<td>Type</td>
<td>Origin from where this group mapping was learned.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ip pim rp-hash 239.1.2.0
RP-Address  192.168.10.1    Type Static
```

If no RP Group mapping exists on the router, the following message is displayed:

No RP-Group mappings exist/learned for the specified group address.
show ip pim rp mapping

The `show ip pim rp mapping` command is used in User Exec and Privileged Exec modes to display the mappings for the PIM group to the active rendezvous points.

**Syntax**

```
show ip pim rp mapping [rp-address | candidate | static]
```

rp-address — An RP address.

**Default configuration**

There is no default configuration for this command.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>Address of the RP</td>
</tr>
<tr>
<td>Group Address</td>
<td>Address of the multicast group.</td>
</tr>
<tr>
<td>Group Mask</td>
<td>Mask for the group address.</td>
</tr>
<tr>
<td>Origin</td>
<td>Origin from where this group mapping is learned.</td>
</tr>
</tbody>
</table>

**Example**

```
console#show ip pim rp mapping candidate
RP Address................................. 192.168.10.1
   Group Address............................ 224.1.2.1
   Group Mask............................... 255.255.0.0
   Origin.................................... BSR
   C-RP Advertisement Interval (secs)....... 60
   Next Candidate RP Advertisement (hh:mm:ss). 00:00:15
```

If no RP Group mapping exists on the router, the following message is displayed:
No RP-Group mappings exist on this router.

If no static RP Group mapping exists on the router, the following message is displayed:

No Static RP-Group mappings exist on this router.

**show ip pim statistics**

Use the `show ip pim statistics` command to display the count of PIM sparse mode received control packets per VLAN.

**Syntax**

```
show ip pim statistics [vlan vlan-id]
```

`vlan-id` — The VLAN for which PIM sparse mode statistics are displayed.

**Default configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec modes, Global Configuration mode and all submodes

**User Guidelines**

This command only displays output if pim sparse-mode is enabled.

The following statistics are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stat</td>
<td>Rx: Packets received.</td>
</tr>
<tr>
<td></td>
<td>Tx: Packets transmitted.</td>
</tr>
<tr>
<td>Interface</td>
<td>The PIM enabled routing interface.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of PIM Hello messages.</td>
</tr>
<tr>
<td>Register</td>
<td>Number of PIM Register messages.</td>
</tr>
<tr>
<td>Reg-Stop</td>
<td>Number of PIM Register-Stop messages.</td>
</tr>
<tr>
<td>Join/Pru</td>
<td>Number of PIM Join/Prune messages.</td>
</tr>
<tr>
<td>BSR</td>
<td>Number of PIM Boot Strap messages.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Assert | Number of PIM Assert messages
CRP | Number of PIM Candidate RP Advertisement messages.

### Example
```
console#show ip pim statistics
=====================================================================  
Interface Stat Hello Register Reg-Stop Join/Pru BSR Assert CRP
=====================================================================  
Vl10  Rx  0  0  0  0  0  0  0 0  0  0  0  0
    Tx  2  0  0  0  0  0  0  0 0  0  0  0  0
Invalid Packets Received - 0
---------------------------------------------------------------------  
Vl20  Rx  0  0  0  5  0  0  0 0  0  0  0  0
    Tx  8  7  0  0  0  0  0  0 0  0  0  0  0
Invalid Packets Received - 0
---------------------------------------------------------------------  
```

```
console#show ip pim statistics vlan 10
=====================================================================  
Interface Stat Hello Register Reg-Stop Join/Pru BSR Assert CRP
=====================================================================  
Vl10  Rx  0  0  0  0  0  0  0 0  0  0  0  0
    Tx  2  0  0  0  0  0  0  0 0  0  0  0  0
Invalid Packets Received - 0
```
IPv6 Multicast Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

The Dell N1500/N2000/N2100-ON series supports limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear ipv6 mroute</th>
<th>ipv6 pim sparse-mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim (VLAN Interface config)</td>
<td>ipv6 pim ssm</td>
</tr>
<tr>
<td>ipv6 pim bsr-border</td>
<td>show ip mroute group</td>
</tr>
<tr>
<td>ipv6 pim bsr-candidate</td>
<td>show ip mroute source</td>
</tr>
<tr>
<td>ipv6 pim dense-mode</td>
<td>show ipv6 pim</td>
</tr>
<tr>
<td>ipv6 pim dr-priority</td>
<td>show ipv6 pim bsr-router</td>
</tr>
<tr>
<td>ipv6 pim hello-interval</td>
<td>show ipv6 pim interface</td>
</tr>
<tr>
<td>ipv6 pim join-prune-interval</td>
<td>show ipv6 pim neighbor</td>
</tr>
<tr>
<td>ipv6 pim register-threshold</td>
<td>show ipv6 pim rp-hash</td>
</tr>
<tr>
<td>ipv6 pim rp-address</td>
<td>show ipv6 pim rp mapping</td>
</tr>
<tr>
<td>ipv6 pim rp-candidate</td>
<td>show ipv6 pim statistics</td>
</tr>
</tbody>
</table>

**clear ipv6 mroute**

This command is used to selectively clear dynamic IPv6 multicast entries from the cache.

**Syntax**

```plaintext
clear ipv6 mroute { * | group-address [ source-address ] }
```

* — Deletes all IPv6 entries from the IP multicast routing table.

group-address — IPv6 address of the multicast group.

source-address — IPv6 address of a multicast source that is sending multicast traffic to the group.
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command does not clear static multicast route entries.
When a * entry is deleted through this command, it cannot be formed again until it is expired in MLD and started again via the host. The default mcache time-out is 210 seconds.

**Example**
The following example deletes all entries from the IPv6 multicast routing table:

```
console# clear ipv6 mroute *
```

The following example deletes from the IPv6 multicast routing table all entries that match the given multicast group address (FF4E::1), irrespective of which source is sending for this group:

```
console# clear ipv6 mroute FF4E::1
```

The following example deletes from the IPv6 multicast routing table all entries that match the given multicast group address (FF4E::1) and the multicast source address (2001::2):

```
console# clear ipv6 mroute FF4E::1 2001::2
```

**ipv6 pim (VLAN Interface config)**
Use the `ipv6 pim` command in VLAN Interface configuration mode to administratively enable PIM multicast routing mode on a particular IPv6 router interface. Use the `no` form of this command to disable PIM on an interface.

**Syntax**

```
ipv6 pim
```
no ipv6 pim

**Default Configuration**
PIM is disabled by default.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
Either PIM-SM or PIM-DM are enabled by this command depending on the globally configured mode. Refer to the `ipv6 pim sparse-mode` and `ipv6 pim dense-mode` commands for further information.

**Example**
cconsole(config-if-vlan3)#ipv6 pim

**ipv6 pim bsr-border**
Use the `ipv6 pim bsr-border` command to prevent bootstrap router (BSR) messages from being sent or received through an interface. Use the `no` form of this command to disable the interface from being the BSR border.

**Syntax**

ipv6 pim bsr-border
no ipv6 pim bsr-border

**Default Configuration**
BSR-border is disabled by default.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
There are no user guidelines for this command.
Example
console(config-if-vlan3)#ipv6 pim bsr-border

**ipv6 pim bsr-candidate**

Use the `ipv6 pim bsr-candidate` command to configure the router to announce its candidacy as a bootstrap router (BSR). Use the `no` form of this command to stop the router from announcing its candidacy as a bootstrap router.

**Syntax**

```plaintext
ipv6 pim bsr-candidate vlan vlan-id hash-mask-len [priority] [interval]
no ipv6 pim bsr-candidate vlan vlan-id
```

- **vlan-id** — A valid VLAN ID value.
- **hash-mask-len** — The length of a mask that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups. (Range 0–128 bits).
- **priority** — The priority of the candidate BSR. The BSR with the higher priority is preferred. If the priority values are the same, the router with the higher IP address is the BSR. (Range: 0–255).
- **interval** — The interval at which candidate rendezvous point advertisements are sent.

**Default Configuration**

The router will not announce its candidacy by default.
The default hash mask length is 126 bits.
The default priority is 0.
The default C-RP advertisement interval is 60 seconds.

**Command Mode**

Global Configuration mode
User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pim bsr-candidate vlan 9 10 34
```

deny

**ipv6 pim dense-mode**

Use the `ipv6 pim dense-mode` command in Global configuration mode to administratively configure PIM dense mode for IPv6 multicast routing. This command also enables MLD. Use the `no` form of this command to disable PIM and MLD. This command does not affect `ip multicast-routing`.

**Syntax**

```
ipv6 pim dense-mode
no ipv6 pim
```

**Default Configuration**

PIM dense mode is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Only one of sparse or dense mode can be configured on a router. DVMRP must be disabled before enabling PIM.

**Example**

```
console(config)#ipv6 pim dense
```

**ipv6 pim dr-priority**

Use the `ipv6 pim dr-priority` command to set the priority value for which a router is elected as the designated router (DR). Use the `no` form of this command to set the priority to the default.
**Syntax**

ipv6 pim dr-priority priority
no ipv6 pim dr-priority

- priority — The election priority (Range: 0–2147483647).

**Default Configuration**

The default election priority is 1.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config-if-vlan3)#ipv6 pim dr-priority 10
```

**ipv6 pim hello-interval**

Use the `ipv6 pim hello-interval` command to configure the PIM-SM Hello Interval for the specified interface. Use the `no` form of this command to set the hello interval to the default.

**Syntax**

ipv6 pim hello-interval interval
no ipv6 pim hello-interval

- interval — The hello interval (Range: 0–18000 seconds).

**Default Configuration**

The default hello interval is 30 seconds.

**Command Mode**

Interface Configuration (VLAN) mode
User Guidelines
Setting the hello interval to 0 disables sending on PIM Hellos.

Example
console(config-if-vlan3)#ipv6 pim hello-interval 45

ipv6 pim join-prune-interval
Use the ipv6 pim join-prune-interval command to configure the interface join/prune interval for the PIM-SM router. Use the no form of this command to set the join/prune interval to the default.

Syntax
ipv6 pim join-prune-interval interval
no ipv6 pim join-prune-interval
  •  interval—The join/prune interval (Range: 0–18000 seconds).

Default Configuration
The default join/prune interval is 60 seconds.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
There are no user guidelines for this command.

Example
console(config-if-vlan3)#ipv6 pim join-prune-interval 90

ipv6 pim register-threshold
Use the ipv6 pim register-threshold command to configure the Register Threshold rate for the RP router to switch to the shortest path. Use the no form of this command to set the register threshold rate to the default.
Syntax

ipv6 pim register-threshold threshold
no ipv6 pim register-threshold
  • threshold—The threshold rate (Range: 0–2000 Kbps).

Default Configuration
The default threshold rate is 0.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example

console(config)#ipv6 pim register-threshold 250

ipv6 pim rp-address

Use the ipv6 pim rp-address command to statically configure the RP address for one or more multicast groups. The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR. Use the no form of this command to remove the RP address for one or more multicast groups.

Syntax

ipv6 pim rp-address rp-address group-address/prefixlength [ override ]
no ipv6 pim rp-address rp-address group-address/prefixlength
  • rp-address—An RP address.
  • group-address—The group address to display.
  • prefixlength—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–128)
Default Configuration
There are no static RP addresses configured by default.

Command Mode
Global Configuration mode

User Guidelines
There are no user guidelines for this command.

Example
console(config)#ipv6 pim rp-address 2001::1 ff1e::/64

ipv6 pim rp-candidate
Use the ipv6 pim rp-candidate command to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR). Use the no form of this command to disable the router from advertising itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Syntax
ipv6 pim rp-candidate vlan vlan-id group-address/prefixlength [interval c_rp_interval ]
no ipv6 pim rp-candidate vlan vlan-id
  •  vlan-id—A valid VLAN ID value.
  •  group-address—The group address to display.
  •  prefixlength—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–128)
  •  c_rp_interval—The Candidate RP advertisement interval (range 1-16383 seconds, default 60 seconds).

Default Configuration
The router does not advertise itself as a PIM candidate rendezvous point by default.
**Command Mode**
Global Configuration mode

**User Guidelines**
The default interval for a Candidate Rendezvous Point (C-RP) to send C-RP Advertisement messages to the Bootstrap Router (BSR) is 60 seconds.

**Example**
```
console(config)#ipv6 pim rp-candidate vlan 6 ff1e::/64
```

**ipv6 pim sparse-mode**
Use the `ipv6 pim sparse-mode` command to administratively configure PIM sparse mode for multicast routing. This command also enables MLD. Use the `no` form of this command to disable PIM and MLD.

**Syntax**
```
ipv6 pim sparse-mode
no ipv6 pim
```

**Default Configuration**
IPv6 PIM sparse mode is disabled by default.

**Command Mode**
Global Configuration mode

**User Guidelines**
Only one of sparse or dense mode can be configured on a router. DVMRP must be disabled before enabling PIM.

**Example**
```
console(config)#ipv6 pim sparse-mode
```
**ipv6 pim ssm**

Use the `ipv6 pim ssm` command to define the Source Specific Multicast (SSM) range of multicast addresses.

### Syntax

`ipv6 pim ssm {default | group-address/prefixlength}
- **default** — Defines the SSM range access list to FF3x::/32.
- **group-address** — Group IP address supported by RP.
- **prefixlength** — This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–128)

### Default Configuration

The default range is FF3x::/32.

### Command Mode

Global Configuration mode

### User Guidelines

There are no user guidelines for this command.

### Example

```
console(config)#ipv6 pim ssm ff1e::/64
```

**show ipv6 pim**

Use the `show ipv6 pim` command to display global status of IPv6 PIMSM and its IPv6 routing interfaces.

### Syntax

```
show ipv6 pim
```

### Default Configuration

There is no default configuration for this command.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```
console(config)#show ipv6 pim
PIM Mode........................................ Sparse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface-Mode</th>
<th>Operational-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vl1</td>
<td>Enabled</td>
<td>Operational</td>
</tr>
</tbody>
</table>
```

**show ipv6 pim bsr-router**
Use the `show ipv6 pim bsr-router` command to display the bootstrap router (BSR) information.

**Syntax**
```
show ipv6 pim bsr-router { candidate | elected }
```
- candidate—Show the IPv6 PIM candidate bootstrap router information.
- elected—Show the IPv6 elected PIM bootstrap router information.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**
Field descriptions are shown in the following table.
### Layer 3 Routing Commands

#### Example

```plaintext
console(config)#show ipv6 pim bsr-router candidate

BSR Address.................................... 2001:0db8:0:badc::1
BSR Priority................................. 0
BSR Hash Mask Length......................... 64
C-BSR Advertisement Interval (secs).......... 60
Next Bootstrap message (hh:mm:ss)............ 00:00:32

If no configured/elected BSR’s exist on the router, the following message is displayed:

No BSR’s exist/learned on this router.
```
**show ipv6 mroute**

Use the `show ipv6 mroute` command to display a summary or all the details of the multicast table.

**Syntax**

`show ipv6 mroute [group groupip [summary] | source sourceip [summary] | static summary]`

- **group**—Show the multicast route information for the specified multicast group.
- **source**—Show the multicast route information for the specified multicast source.
- **static**—Show the multicast route information for the specified static multicast group.
- **summary**—Summarize the information.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show ipv6 mroute summary

Multicast Route Table Summary

Source IP Group IP Protocol IIF OIF Expiry
--------------- --------------- -------- --------- -------
* FF43::5 PIMSM Vl11 Vl11
2001::5 FF43::5 PIMSM Vl12 Vl11
2001::5 FF43::5 PIMSM Vl13 Vl13

console#show ipv6 mroute summary
```
### Multicast Route Table Summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>IIF</th>
<th>OIF</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>Vl11</td>
<td>Vl13</td>
<td></td>
</tr>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>Vl12</td>
<td>Vl11</td>
<td>Vl13</td>
</tr>
</tbody>
</table>

```
console#show ipv6 mroute source 2001::5 ?
<cr>
Press enter to execute the command.
|                        Output filter options.
| summary                Display the IPV6 multicast routing table summary.
```

```
console#show ipv6 mroute source 2001::5
```

```
Multicast Route Table

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Expiry (mm:ss)</th>
<th>Up Time (hh:mm:ss)</th>
<th>RPF Neighbor</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>03:08</td>
<td>00:00:21</td>
<td>2001::5</td>
<td>SPT</td>
</tr>
</tbody>
</table>
```

```
console#show ipv6 mroute source 2001::5 summary
```

```
Multicast Route Table Summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>IIF</th>
<th>OIF</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>Vl12</td>
<td>Vl11</td>
<td>Vl13</td>
</tr>
</tbody>
</table>
```

```
console#show ipv6 mroute group FF43::5 ?
<cr>
Press enter to execute the command.
|                        Output filter options.
| summary                Display the IPV6 multicast routing table summary.
```

```
console#show ipv6 mroute group FF43::5
```

```
Multicast Route Table

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Expiry (mm:ss)</th>
<th>Up Time (hh:mm:ss)</th>
<th>RPF Neighbor</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>FF43::5</td>
<td>00:00</td>
<td>00:01:00</td>
<td>::</td>
<td>RPT</td>
</tr>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>02:54</td>
<td>00:00:35</td>
<td>2001::5</td>
<td>SPT</td>
</tr>
</tbody>
</table>
```

```
console#show ipv6 mroute group FF43::5 summary
```

```
Multicast Route Table Summary
```
show ipv6 mroute group

Use the `show ipv6 mroute group` command to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the groupipaddr value.

**Syntax**

```
show ipv6 mroute group groupipaddr [summary]
```

- `groupipaddr` — IP address of the multicast group.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show ipv6 mroute group FF43::5 ?
<cr> Press enter to execute the command.
| summary Display the IPV6 multicast routing table summary.
```

```
console#show ipv6 mroute group FF43::5

Multicast Route Table

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Expiry (mm:ss)</th>
<th>Up Time (hh:mm:ss)</th>
<th>RPF Neighbor</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>V111</td>
<td>V113</td>
<td></td>
</tr>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>V112</td>
<td>V111</td>
<td></td>
</tr>
</tbody>
</table>
```
show ipv6 mroute source

Use the `show ipv6 mroute source` command to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the sourceipaddr or sourceipaddr | groupipaddr pair value(s).

**Syntax**

```
show ipv6 mroute source sourceipaddr {summary | groupipaddr}
```

- `sourceipaddr` — IP address of source.
- `groupipaddr` — IP address of multicast group.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show ipv6 mroute source 2001::5 ?
```
Press enter to execute the command.

Output filter options.

| summary | Display the IPv6 multicast routing table summary.

```
console#show ipv6 mroute source 2001::5

Multicast Route Table

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Expiry (mm:ss)</th>
<th>Up Time (hh:mm:ss)</th>
<th>RPF Neighbor</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>03:08</td>
<td>00:00:21</td>
<td>2001::5</td>
<td>SPT</td>
</tr>
</tbody>
</table>

console#show ipv6 mroute source 2001::5 summary

Multicast Route Table Summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>IIF</th>
<th>OIF</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::5</td>
<td>FF43::5</td>
<td>PIMSM</td>
<td>V112</td>
<td>V111</td>
<td>V113</td>
</tr>
</tbody>
</table>
```

**show ipv6 pim interface**

Use the `show ipv6 pim interface` command to display interface config parameters. If no interface is specified, all interfaces are displayed.

**Syntax**

```
show ipv6 pim interface [vlan vlan-id]
```

- vlan-id—A valid VLAN ID value.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.
Example

```console
console#show ipv6 pim interface vlan 6
Slot/Port................................. vlan 6
IP Address................................ FE80::2FF:EDFF:FED0:2/128
Hello Interval (secs)..................... 30
Join Prune Interval (secs)................. 60
Neighbor Count............................ 0
Designated Router......................... FE80::2FF:EDFF:FED0:2
DR Priority................................ 1
BSR Border................................ Disabled
```

**show ipv6 pim neighbor**

Use the `show ipv6 pim neighbor` command to display IPv6 PIMSM neighbors learned on the routing interfaces.

**Syntax**

```
show ipv6 pim neighbor [interface vlan vlan-id ]
```

- `vlan-id` — A valid VLAN ID value.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

If a VLAN interface is not specified, all neighbors are shown.

**Example**

```console
console#show ipv6 pim neighbor
Slot/Port................................. vlan 6
Neighbor Address.......................... FE80::200:FF:FE00:33
Up Time (hh:mm:ss).......................... 00:00:12
Expiry Time (hh:mm:ss)...................... 00:01:34
DR Priority................................ 0
```
**show ipv6 pim rp-hash**

Use the `show ipv6 pim rp-hash` command to display which rendezvous point (RP) is being selected for a specified group.

**Syntax**

```
show ipv6 pim rp-hash group-address
```

`group-address`—Group IP address supported by RP.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console#show ipv6 pim rp-hash ff1e::/64
```

<table>
<thead>
<tr>
<th>RP Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3001::1</td>
<td>BSR</td>
</tr>
</tbody>
</table>

**show ipv6 pim rp mapping**

Use the `show ipv6 pim rp mapping` command to display all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR). If no RP is specified, all active RPs are displayed.

**Syntax**

```
show ipv6 pim rp mapping [ rp-address | candidate | static ]
```

- `rp-address`—IP address of RP.
- `candidate`—Show candidate rendezvous point mappings.
• static—Show static rendezvous point mappings.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Example**
```console
console#show ipv6 pim rp mapping
Group Address.................................. FF1E::/64
RP Address..................................... 2001::1
origin......................................... Static
Group Address.................................. FF1E::/64
RP Address..................................... 3001::1
origin......................................... BSR
```

**show ipv6 pim statistics**
Use the `show ipv6 pim statistics` command to display the count of IPv6 PIM sparse mode received control packets.

**Syntax**
```plaintext
show ipv6 pim statistics [ vlan vlan-id ]
```
- `vlan vlan-id`—The VLAN for which to display sparse mode statistics.

**Default Configuration**
This command has no defaults.

**Command Mode**
Privileged Exec mode, Global Configuration mode, all sub-modes.
**User Guidelines**

This command only displays output if pim sparse-mode is enabled. The following counters are displayed in the output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stat</td>
<td>Rx: Packets received.</td>
</tr>
<tr>
<td></td>
<td>Tx: Packets transmitted.</td>
</tr>
<tr>
<td>Interface</td>
<td>The PIM enabled routing interface.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of PIM Hello messages.</td>
</tr>
<tr>
<td>Register</td>
<td>Number of PIM Register messages.</td>
</tr>
<tr>
<td>Reg-Stop</td>
<td>Number of PIM Register-Stop messages.</td>
</tr>
<tr>
<td>Join/Prune</td>
<td>Number of PIM Join/Prune messages.</td>
</tr>
<tr>
<td>BSR</td>
<td>Number of PIM Boot Strap messages.</td>
</tr>
<tr>
<td>Assert</td>
<td>Number of PIM Assert messages.</td>
</tr>
<tr>
<td>CRP</td>
<td>Number of PIM Candidate RP Advertisement messages.</td>
</tr>
</tbody>
</table>

**Example**

```console
console#show ipv6 pim statistics
===================================================================== 
Interface Stat  Hello Register Reg-Stop Join/Prune BSR  Assert  CRP
===================================================================== 
Vl10  Rx       0        0        0        0     0     0     0     0
      Tx       2        0        0        0     0     0     0
Invalid Packets Received - 0
Vl20  Rx       0        0        0        5     0     0     0     0
      Tx       8        7        0        0     0     0     0
Invalid Packets Received - 0
Gi1/0/5 Rx     0        0        6        5     0     0     0     0
      Tx     10        9        0        0     0     0     0
Invalid Packets Received - 0

console#show ipv6 pim statistics vlan 10
======================================================================
Interface Stat  Hello Register Reg-Stop Join/Prune BSR  Assert  CRP
======================================================================
```
<table>
<thead>
<tr>
<th>Vl10</th>
<th>Rx</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>2</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tx</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Invalid Packets Received - 0
OSPF Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

The Dell Network N1500/N2000/N2100-ON series support limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.

OSPF is a link-state protocol. Dell EMC Networking OSPF supports variable-length subnet masks. Dell EMC Networking OSPF only operates over VLAN interfaces.

OSPF operates within a hierarchy. The largest entity within the hierarchy is the autonomous system (AS), a collection of networks under a common administration sharing a common routing strategy. This is sometimes called a routing domain. An AS can be divided into a number of areas or groups of contiguous networks and attached hosts. Routers within the same area share the same information, so they have identical topological databases.

Information is sent in the form of link-state advertisements (LSAs) to all other routers within the same hierarchical area. An area's topology is not visible to routers outside the area.

Two different types of OSPF routing occur as a result of area partitioning: Intra-area and Inter-area. Intra-area routing occurs if a source and destination are in the same area. Inter-area routing occurs when a source and destination are in different areas. An OSPF backbone distributes information between areas.

For IPv4 networks, Dell EMC Networking routing supports OSPF version 2 in accordance with RFC 2328. The Dell EMC Networking routing also provides a compatibility mode for the RFC 1583 OSPF specification, which allows interoperability with OSPF version 2 routers using the older implementation.

The Dell EMC Networking OSPFv2 implementation supports point-to-point operation on Ethernet interfaces. The user can configure an OSPFv2 interface to run in broadcast or point-to-point mode. When there are only two routers attached to the link, OSPFv2 point-to-point mode has the advantage of not requiring designated router election or origination of a network LSA for the LAN. This makes the protocol more efficient. Dell EMC Networking also supports OSPFv3 for use with IPv6 networks.

The Dell EMC Networking routing OSPF NSSA feature supports RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option.
Route Preferences

Normally, OSPF select routes in the following order:

- Local
- Static
- Intra-area
- Inter-area
- External
- RIP

Dell EMC Networking OSPF allows the administrator to change the preference for selecting intra, inter, and external routes according to the following rules:

a. External route preferences apply to all ospf external routes like type1, type2, nssa-type1, nssa-type2 equally.

b. Multiple route types may be configured with equal preference values.

c. Configuring a route preference of 255 makes the route ineligible to be selected as the best route to its destination. That is, a route type with a preference of 255 shall never be used for forwarding.

The RIP preference is not used in IPv6 routing.

OSPF Equal Cost Multipath (ECMP)

A device running the IP routing protocol OSPF maintains multiple equal-cost routes to all destinations. The multiple routes are of the same type (intra-area, inter-area, type 1 external or type 2 external), cost, and have the same associated area. However, each route is defined by a separate advertising router and next hop.

With ECMP, a device forwards traffic to a specified destination through multiple paths thereby taking advantage of the bandwidth of both links.

ECMP routes are configured statically or learned dynamically as follows:

- Configured Statically: If an operator configures multiple static routes to the exact same destination but with different next hops, those routes are treated as a single route with two next hops.
• Learned Dynamically: Routing protocols can learn ECMP routes. For example, if OSPF is configured on both links connecting Router A to Router B with interface addresses 10.1.1.2 and 10.1.2.2 respectively, and Router B advertises its connection to 20.0.0.0/8, then Router A computes an OSPF route to 20.0.0.0/8 with next hops of 10.1.1.2 and 10.1.2.2.

Dell EMC Networking routing stores static and dynamic routes in a single combined routing table. RTO accepts ECMP routes, but it is important to understand that RTO does not combine routes from different sources to create ECMP routes. Referring to the above configuration, assume OSPF is only configured on the 10.1.1.2 Router B interface connecting Router A and Router B. Then on Router A, OSPF reports to RTO a route to 20.0.0.0/8 with a next hop of 10.1.1.2. If the user configures a static route to 20.0.0.0/8 with a single next hop of 10.1.2.2, RTO does NOT combine the OSPF and static route into a single route to 20.0.0.0/8 with two next hops. All next hops within an ECMP route must be provided by the same source.

On Dell EMC Networking N3000, N3100, and N4000 platforms, the ECMP hashing support utilizes Enhanced hashing mode, which provides improved load-balancing performance. ECMP hashing on these platforms has the following features:

• MODULO-N operation based on the number N of next hops in the route.
• Packet attributes selection based on the packet type. For IP packets, the following fields are used: Source IP address, Destination IP address, TCP/UDP port, IPv4 Protocol, IPv6 next header.

**Forwarding of OSPF Opaque LSAs Enabled by Default**

Dell EMC Networking supports the flooding capability of opaque LSAs. Dell EMC Networking cannot originate or process opaque LSAs. In the past, the capability to flood opaque LSAs was disabled by default.

**Passive Interfaces**

The passive interface feature is used to disable sending OSPF routing updates on an interface. An OSPF adjacency will not be formed on such an interface. On a passive interface, subnet prefixes for IP addresses configured on the interface will continue to be advertised as stub networks.
Graceful Restart

The Dell EMC Networking implementation of OSPFv2 supports graceful restart as specified in RFC 3623. Graceful restart works in concert with Dell EMC Networking nonstop forwarding to enable the hardware to continue forwarding IPv4 packets using OSPFv2 routes while a backup unit takes over management unit responsibility. When OSPF executes a graceful restart, it informs its neighbors that the OSPF control plane is restarting, but that it will be back shortly. Helpful neighbors continue to advertise to the rest of the network that they have full adjacencies with the restarting router, avoiding announcement of a topology change and everything that goes with that (i.e., flooding of LSAs, SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Dell EMC Networking implements both the restarting router and helpful neighbor features described in RFC 3623.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area default-cost (Router OSPF)</td>
<td>capability opaque</td>
</tr>
<tr>
<td>area nssa (Router OSPF)</td>
<td>clear ip ospf</td>
</tr>
<tr>
<td>area nssa default-info originate (Router OSPF Config)</td>
<td>clear ip ospf stub-router</td>
</tr>
<tr>
<td>area nssa no-redistribute</td>
<td>compatible rfc1583</td>
</tr>
<tr>
<td>area nssa no-summary</td>
<td>default-information originate (Router OSPF Configuration)</td>
</tr>
<tr>
<td>area nssa translator-role</td>
<td>default-metric max-metric router-lsa</td>
</tr>
<tr>
<td>ip ospf network</td>
<td>show ip ospf area</td>
</tr>
<tr>
<td>ip ospf priority</td>
<td>show ip ospf asbr</td>
</tr>
<tr>
<td>ip ospf retransmit-interval</td>
<td>show ip ospf database</td>
</tr>
<tr>
<td>ip ospf transmit-delay</td>
<td>show ip ospf database database-summary</td>
</tr>
<tr>
<td>log adjacency-changes</td>
<td>show ip ospf interface database-summary</td>
</tr>
<tr>
<td>max-metric router-lsa</td>
<td>show ip ospf interface brief</td>
</tr>
</tbody>
</table>
area nssa translator-stab-intv
distance ospf
distance ospf maximum-paths
maximum-paths show ip ospf interface stats
show ip ospf interface stats
area range (Router OSPF)
distribute-list out
distribute-list out network area
network area show ip ospf lsa-group
show ip ospf lsa-group
area stub
enable
enable nsf
nsf show ip ospf neighbor
show ip ospf neighbor
area stub no-summary
exit-overflow-interval
exit-overflow-interval nsf helper
nsf helper show ip ospf range
show ip ospf range
area virtual-link
external-lsdb-limit
external-lsdb-limit nsf helper strict-lsa-checking
nsf helper strict-lsa-checking show ip ospf statistics
show ip ospf statistics
area virtual-link authentication
ip ospf area
ip ospf area nsf restart-interval
nsf restart-interval show ip ospf stub table
show ip ospf stub table
area virtual-link dead-interval
ip ospf authentication
ip ospf authentication passive-interface
passive-interface show ip ospf traffic
passive-interface show ip ospf virtual-links
show ip ospf virtual-links
area virtual-link hello-interval
ip ospf cost
ip ospf cost passive-interface
default show ip ospf virtual-links
show ip ospf virtual-links
area virtual-link retransmit-interval
ip ospf database-filter all out
distribute (BGP) redistribute (BGP) show ip ospf virtual-links brief
show ip ospf virtual-links brief
area virtual-link transmit-delay
ip ospf dead-interval
ip ospf dead-interval router-id
timer pacing flood
timer pacing flood
auto-cost
ip ospf hello-interval
ip ospf hello-interval router ospf
timer pacing lsa-group
timer pacing lsa-group
bandwidth
ip ospf mtu-ignore
ip ospf mtu-ignore show ip ospf
show ip ospf timers spf
timer spf
timer spf
bfd
–
– show ip ospf abr
show ip ospf abr

**area default-cost (Router OSPF)**

Use the `area default-cost` command in Router OSPF Configuration mode to configure the advertised default cost for the stub area. Use the `no` form of the command to return the cost to the default value.

**Syntax**

```
area area-id default-cost integer
no area area-id default-cost
```
• area-id — Identifies the OSPF stub area to configure. (Range: IP address or decimal from 0-4294967295)
• integer — The default cost for the stub area. (Range: 1–16777215)

Default Configuration
10 is the default configuration for integer.

Command Mode
Router OSPF Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example identifies a stub area of 10 and default cost of 100.

```
console(config)#router ospf
console(config-router)#area 10 default-cost 100
```

area nssa (Router OSPF)

Use the `area nssa` command in Router OSPF Configuration mode to configure the specified area ID to function as an NSSA. If the area has not been previously created, this command creates the area and then applies the NSSA distinction. If the area already exists, the NSSA distinction is added or modified. Use the `no` form of the command to remove the NSSA distinction from the specified area ID.

Syntax

```
area area-id nssa [no-redistribution] [default-information-originate [metric metric-value] [metric-type metric-type-value]] [no-summary] [translator-role role] [translator-stab-intv interval]
no area area-id nssa [no-redistribution] [default-information-originate] [no-summary] [translator-role] [translator-stab-intv]
```

• area-id—Identifies the OSPF stub area to configure. (Range: IP address or decimal from 0–4294967295)
• **metric-value**—Specifies the metric of the default route advertised to the NSSA. (Range: 1–16777214)

• **metric-type-value**—The metric type can be one of the following:
  – A metric type of nssa-external 1
  – A metric type of nssa-external 2 (default)

• **role**—The translator role where role is one of the following:
  – always - The router assumes the role of the translator when it becomes a border router.
  – candidate - The router to participate in the translator election process when it attains border router status.

• **interval**—The period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. (Range: 0–3600)

**Default Configuration**

If no metric is defined, 10 is the default configuration.
The default role is candidate. The default metric is type 2.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

Specifying a metric with no metric type is equivalent to specifying a metric with a metric type of 2.

**Example**

The following example configures not-so-stubby-area 10 as an NSSA.

```
c console(config)#router ospf
c console(config-router)#area 10 nssa
```

The following example configures the metric value and type for the default route advertised into the NSSA and configures the NSSA so that summary LSAs are not advertised into the NSSA.

```
c console(config-router)#area 20 nssa default-info-originate metric 250 metric-type 2 no-summary
```
**area nssa default-info-originate (Router OSPF Config)**

Use the `area nssa default-info-originate` command in Router OSPF Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2). Use the no form of the command to return the metric value and type to the default value.

**Syntax**

```plaintext
area area-id nssa default-info-originate [integer] [comparable | non-comparable]
no area area-id nssa default-info-originate
```

- **area-id** — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- **integer** — Specifies the metric of the default route advertised to the NSSA. (Range: 1–16777214)
- **comparable** — A metric type of nssa-external 1
- **non-comparable** — A metric type of nssa-external 2

**Default Configuration**

If no metric is defined, 10 is the default configuration.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures the metric value and type for the default route advertised into the NSSA.

```plaintext
console(config-router)#area 20 nssa default-info-originate 250 non-comparable
```
area nssa no-redistribute

Use the area nssa no-redistribute command in Router OSPF Configuration mode to configure the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.

Syntax

area area-id nssa no-redistribute
no area area-id nssa no-redistribute

• area-id — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the NSSA ABR.

console(config-router)#area 20 nssa no-redistribute

area nssa no-summary

Use the area nssa no-summary command in Router OSPF Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA.

Syntax

area area-id nssa no-summary
no area area-id nssa no-summary

• area-id — Identifies the OSPF NSSA to configure. (Range: 0–4294967295)
Default Configuration
This command has no default configuration.

Command Mode
Router OSPF Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example configures the NSSA so that summary LSAs are not advertised into the NSSA.

console(config-router)#area 20 nssa no-summary

area nssa translator-role
Use the area nssa translator-role command in Router OSPF Configuration mode to configure the translator role of the NSSA.

Syntax
area area-id nssa translator-role {always | candidate}
no area area-id nssa translator-role

- area-id — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- always — The router assumes the role of the translator when it becomes a border router.
- candidate — The router to participate in the translator election process when it attains border router status.

Default Configuration
The default role is candidate.

Command Mode
Router OSPF Configuration mode.
User Guidelines
This command has no user guidelines.

Example
The following example configures the translator role of the NSSA.
console(config-router)#area 20 nssa translator-role always

area nssa translator-stab-intv
Use the area nssa translator-stab-intv command in Router OSPF Configuration mode to configure the translator stability interval of the NSSA.

Syntax
area area-id nssa translator-stab-intv integer
no area area-id nssa translator-stab-intv

• area-id — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
• integer — The period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. (Range: 0–3600)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPF Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example configures the translator stability interval of the area 20 NSSA.
console(config-router)#area 20 nssa translator-stab-intv 2000
area range (Router OSPF)

Use the area range command in Router OSPF Configuration mode to configure a summary prefix that an area border router advertises for a specific area. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA.

Use the no form of the command to delete an area range or revert an option to its default.

Syntax

```
area area-id range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise][cost cost]
```

```
no area area-id range prefix netmask {summarylink | nssaexternallink}
```

- **area-id** — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- **prefix netmask** — The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
- **summarylink** — When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
- **nssaexternallink** — When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
- **advertise** — [Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
- **not-advertise** — [Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. Then the not-advertise option is given, any static cost previously configured is removed from the system configuration.
- **cost** — [Optional] If an optional cost is given, OSPF sets the metric field in the summary LSA to the configured value, rather than setting the metric to the largest cost among the networks covered by the area range. A static cost may only be configured if the area range is configured to advertise the summary. The range is 0 to 16,777,215. If the cost is set to 16,777,215 for type 3 summarization, a
type 3 summary LSA is not advertised, but contained networks are suppressed. This behavior is equivalent to specifying the not-advertise option. If the range is configured for type 7 to type 5 translation, a type 5 LSA is sent if the metric is set to 16,777,215; however, other routers will not compute a route from a type 5 LSA with this metric.

**Default Configuration**

No area ranges are configured by default. No cost is configured by default.

**Command Mode**

OSPFv2 Router Configuration mode

**User Guidelines**

The no form of this command can be used to delete an area range. For example:

```
!! Create area range
console (config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink
!! Delete area range
console (config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink
```

The no form may be used to revert the [advertise | not-advertise] option to its default without deleting the area range. Deleting and recreating the area range would cause OSPF to temporarily advertise the prefixes contained within the range. Note that using either the advertise or not-advertise keyword reverts the configuration to the default. For example:

```
!! Create area range. Suppress summary.
console (config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
!! Advertise summary.
console (config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
```

The no form may be used to remove a static area range cost, so that OSPF sets the cost to the largest cost among the contained routes. For example:

```
!! Create area range with static cost.
console (config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink cost 1000
!! Remove static cost.
console (config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink cost
```
If the user tries to configure both types of ranges for the same prefix and area:

A T3 range with the same prefix is already configured on this area.

If the network mask is invalid:

```console
console (config-router)#area 1 range 0.0.0.0 0.0.0.0 summarylink
An area range mask must have contiguous ones and be no longer than 31 bits.
```

If the prefix is not a valid area range prefix:

```console
console (config-router)#area 1 range 0.0.0.0 255.0.0.0 summarylink
Cannot create this area range because it represents a default route.
```

```console
console (config-router)#area 1 range 225.0.0.0 255.0.0.0 summarylink
225.0.0.0 255.0.0.0 is an invalid prefix for an area range.
```

If the maximum number of ranges is already configured:

```console
console (config-router)#area 3 range 90.0.0.0 255.0.0.0 summarylink cost 50
The maximum number of area ranges (60) is already configured.
```

If the user tries to delete an area range that does not exist:

```console
console (config-router)#no area 4 range 40.0.0.0 255.0.0.0 summarylink
Delete failed. No matching area range configured.
```

**Example**

The following example defines an area range for the area 20.

```console
console(config-router)#area 20 range 192.168.6.0 255.255.255.0 summarylink advertise
```

**area stub**

Use the `area stub` command in Router OSPF Configuration mode to create a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS
External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area. Use the no form of the command to remove the stub area.

**Syntax**

area area-id stub

no area area-id stub

- area-id — Identifies the area identifier of the OSPF stub. (Range: IP address or decimal from 0–4294967295)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

Use the `area stub no-summary` command, in conjunction with this command, to create a totally stubby area.

**Examples**

The following examples define area 3 for the stub and then removes the stub area.

```
console(config-router)#area 3 stub
console(config-router)#no area 3 stub
```

**area stub no-summary**

Use the `area stub no-summary` command in Router OSPF Configuration mode to prevent Summary LSAs from being advertised into the NSSA. Use the no form of the command to return the Summary LSA mode to the default value.

**Syntax**

area area-id stub no-summary
no area area-id stub no-summary

- area-id — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

This command creates a totally stubby area when used in conjunction with the area stub command.

**Example**

The following example prevents the Summary LSA from being advertised into the area 3 NSSA. Area 3 will be configured as a totally stubby area.

```
console(config-router)#area 3 stub
console(config-router)#area 3 stub no-summary
```

**area virtual-link**

Use the area virtual-link command in Router OSPF Configuration mode to create the OSPF virtual interface for the specified area-id and neighbor router. To remove the link, use the no form of the command. Use the optional parameters to configure authentication, dead-interval, hello-interval, retransmit-interval and transmit-delay. If the area has not been previously created, it is created by this command. If the area already exists, the virtual-link information is added or modified.

**Syntax**

```
area area-id virtual-link router-id [authentication [message-digest | null]] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [[authentication-key key] [message-digest-key key-id md5 key]]
```
Layer 3 Routing Commands

no area area-id virtual-link router-id [authentication [message-digest | null]]
[hello-interval] [retransmit-interval] [transmit-delay] [dead-interval]
[[authentication-key] | [message-digest-key]]

- area-id—Identifies the OSPF stub area to configure. (Range: IP address or
decimal from 0-4294967295)
- router-id—Valid IP address.
- authentication—Specifies authentication type.
- message-digest —Specifies that message-digest authentication is used.
- null—No authentication is used. Overrides password or message-digest
authentication if configured for the area.
- hello-interval seconds—Number of seconds to wait before sending hello
packets to the OSPF virtual interface. (Range: 1–65535)
- dead-interval seconds—Number of seconds to wait before the OSPF
virtual interface on the virtual interface is assumed to be dead. (Range: 1–
65535)
- retransmit-interval seconds—The number of seconds to wait between
retransmitting LSAs if no acknowledgment is received. (Range: 0–3600)
- transmit-delay seconds—Number of seconds to increment the age of the
LSA before sending, based on the estimated time it takes to transmit from
the interface. (Range: 0–3600)
- md5—Use MD5 Encryption for an OSPF Virtual Link.
- key—Authentication key for the specified interface. (Range: 8 bytes or less
if the authentication type is simple and 16 bytes or less if the type is
encrypt.)
- key-id—Authentication key identifier for the authentication type encrypt.
(Range: 0–255)

Default Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>No area ID is predefined.</td>
</tr>
<tr>
<td>router-id</td>
<td>No router ID is predefined.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>hello-interval seconds</td>
<td>10 seconds</td>
</tr>
<tr>
<td>retransmit-interval seconds</td>
<td>5 seconds</td>
</tr>
<tr>
<td>transmit-delay seconds</td>
<td>1 second</td>
</tr>
<tr>
<td>dead-interval seconds</td>
<td>40 seconds</td>
</tr>
<tr>
<td>authentication-key key</td>
<td>No key is predefined.</td>
</tr>
<tr>
<td>message-digest-key key-id md5</td>
<td>No key is predefined.</td>
</tr>
</tbody>
</table>

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

Unauthenticated interfaces cannot be configured with an authentication key. Use the `area virtual-link authentication` command to enable configuration of an authentication key.

**Example**

The following example establishes a virtual link with a 40-second transmit-delay interval and default values for all other optional parameters:

```plaintext
router ospf
    network 10.50.50.0 0.0.0.255 area 10
    area 10 virtual-link 192.168.2.2 transmit-delay 40
```

The following example establishes a virtual link with MD5 authentication:

```plaintext
router ospf
    network 10.50.50.0 0.0.0.255 area 10
    area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 100 md5 test123
```
area virtual-link authentication

Use the area virtual-link authentication command in Router OSPF Configuration mode to configure the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the authentication type to the default value.

Syntax

area area-id virtual-link neighbor-id authentication [none | simple key | encrypt key key-id]

no area area-id virtual-link neighbor-id authentication

• area-id — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
• neighbor-id — Identifies the Router identifier of the neighbor.
• encrypt — Use MD5 Encryption for an OSPF Virtual Link.
• key — Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is simple and 16 bytes or less if the type is encrypt.)
• key-id — Authentication key identifier for the authentication type encrypt. (Range: 0–255)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

Unauthenticated interfaces cannot be configured with an authentication key. If no parameters are specified after the authentication keyword, then plain-text password authentication is used.

Example

The following example configures the authentication type and key for the area 10 OSPF virtual interface and neighbor ID.
area virtual-link dead-interval

Use the `area virtual-link dead-interval` command in Router OSPF Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router. Use the `no` form of the command to return the dead interval to the default value.

**Syntax**

```plaintext
area area-id virtual-link neighbor-id dead-interval seconds
no area area-id virtual-link neighbor-id dead-interval
```

- **area-id** — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- **neighbor-id** — Identifies the Router ID of the neighbor.
- **seconds** — Number of seconds to wait before the OSPF virtual interface on the virtual interface is assumed to be dead. (Range: 1–2147483647)

**Default Configuration**

40 seconds is the default configuration.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures the dead interval for the area 10 OSPF virtual interface on the virtual interface and neighbor router.

```plaintext
console(config-router)#area 10 virtual-link 192.168.2.2 dead-interval 655555
```
area virtual-link hello-interval

Use the area virtual-link hello-interval command in Router OSPF Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the hello interval to the default value.

Syntax

area area-id virtual-link neighbor-id hello-interval seconds
no area area-id virtual-link neighbor-id hello-interval

- area-id — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- neighbor-id — Identifies the Router ID of the neighbor.
- seconds — Number of seconds to wait before sending hello packets to the OSPF virtual interface. (Range: 1–65535)

Default Configuration

10 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 50-second wait interval.

console(config-router)#area 10 virtual-link 192.168.2.2 hello-interval 50
area virtual-link retransmit-interval

Use the **area virtual-link retransmit-interval** command in Router OSPF Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the retransmit interval to the default value.

**Syntax**

```
area area-id virtual-link neighbor-id retransmit-interval seconds
no area area-id virtual-link neighbor-id retransmit-interval
```

- **area-id** — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- **neighbor-id** — Identifies the Router ID of the neighbor.
- **seconds** — The number of seconds to wait between retransmitting LSAs if no acknowledgment is received. (Range: 0–3600)

**Default Configuration**

The default configuration is 5 seconds.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures a 500-second retransmit wait interval.

```
console(config-router)#area 10 virtual-link 192.168.2.2 retransmit-interval 500
```
area virtual-link transmit-delay

Use the `area virtual-link transmit-delay` command in Router OSPF Configuration mode to configure the transmit delay for the OSPF virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the transmit delay to the default value.

Syntax

```
area area-id virtual-link neighbor-id transmit-delay seconds
no area area-id virtual-link neighbor-id transmit-delay
```

- **area-id** — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- **neighbor-id** — Identifies the Router ID of the neighbor.
- **seconds** — Number of seconds to increment the age of the LSA before sending, based on the estimated time it takes to transmit from the interface. (Range: 0–3600)

Default Configuration

1 second is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 40-second transmit-delay interval.

```
console(config-router)#area 10 virtual-link 192.168.2.2 transmit-delay 40
```

auto-cost

By default, OSPF computes the link cost of each interface from the interface bandwidth. The link cost is computed as the ratio of a “reference bandwidth” to the interface bandwidth (ref_bw / interface bandwidth), where interface
bandwidth is defined by the “bandwidth” command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. To change the reference bandwidth, use the auto-cost command, specifying the reference bandwidth in megabits per second. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

**Syntax**

`auto-cost reference-bandwidth` `ref_bw`

- `ref_bw` — The reference bandwidth in Mbps (Range: 1–4294967).

**Default Configuration**

The default reference bandwidth is 100 Mbps.

**Command Mode**

OSPFv2 or OSPFv3 Router Configuration mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example configures a reference bandwidth of 500 Mbps.

```
console(config-router)#auto-cost reference-bandwidth 500
```

**bandwidth**

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the auto-cost command. For the purpose of the OSPF link cost calculation, the bandwidth command specifies the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface.
**Syntax**

bandwidth bw

- bw — Interface bandwidth in Kbps (Range: 1–1000000).

**Default Configuration**

The default reference bandwidth is 10 Mbps

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example configures the interface bandwidth to 500000 Kbps.

```
console(config-if-vlan1)#bandwidth 500000
```

**bfd**

Use the `bfd` command to enable processing of BFD events by OSPF on all interfaces enabled for BFD. Use the `no` form of the command to ignore BFD events.

**Syntax**

`bfd`

`no bfd`

**Default Configuration**

The processing of BFD events is not enabled by default.

**Command Mode**

Router OSPF Configuration mode, Router OSPFv3 Configuration mode
**User Guidelines**

BFD processing notifies OSPF of layer 3 connectivity issues with the peer. The interface must be a VLAN interface enabled for routing.

BFD event notification must also be enabled in VLAN interface mode in order for processing of BFD events to occur.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

The following example

```
consle#configure
consle(config)#ip routing
consle(config)#interface vlan 3
consle(config-if-vlan3)#ip address 192.168.0.1 /24
consle(config-if-vlan3)#ip ospf area 0
consle(config-if-vlan3)#ip ospf bfd
consle(config-if-vlan3)#exit
consle(config)#router ospf
consle(config-router)#bfd
```

**capability opaque**

Use the `capability opaque` command to enable Opaque Capability on the router. Use the “no” form of this command to disable Opaque Capability.

**Syntax**

`capability opaque`

`no capability opaque`

**Default Configuration**

Opaque Capability is enabled by default.

**Command Mode**

Router Configuration mode.
**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config-router)#capability opaque
```

**clear ip ospf**

Use the `clear ip ospf` command to reset specific OSPF states. If no parameters are specified, OSPF is disabled and then re-enabled.

**Syntax**

```
clear ip ospf [{configuration | redistribution | counters | neighbor [interface vlan vlan-id [neighbor-id]]}] [vrf vrf-name]
```

- **configuration** — Reset the OSPF configuration to factory defaults.
- **redistribution** — Flush all self-originated external LSAs. Reapply the redistribution configuration and re originate prefixes as necessary.
- **counters** — Reset global and interface statistics.
- **neighbor** — Drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be reestablished.
- **interface vlan vlan-id** — Drop adjacency with all neighbors on a specific interface.
- **neighbor-id** — Drop adjacency with a specific router ID on a specific interface.
- **vrf-name** — The name of the VRF instance on which the command operates. If no VRF parameter is given, counters for the default (global) router instance is cleared.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode.
User Guidelines
The VRF identified in the parameter must have been previously created or an error is returned.

Example
The following example shows the options for the clear ip ospf command.

```
clear ip ospf ?
<cr> Press enter to execute the command.
configuration Restore OSPF configuration to defaults
counters Clear OSPF counters
neighbor Bounce all OSPF neighbors
redistribution Flush and re-originate external LSAs
```

Clear ip ospf stub-router
Use the clear ip ospf stub-router command to force OSPF to exit stub router mode when it has automatically entered stub router mode because of a resource limitation.

Syntax
```
clear ip ospf stub-router [vrf vrf-name]
```

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, counters for the default (global) router instance is cleared.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode

User Guidelines
OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or if it is in stub router mode at startup. This command has no effect if OSPF is configured to be in stub router mode permanently.

The VRF identified in the parameter must have been previously created or an error is returned.
**compatible rfc1583**

Use the `compatible rfc1583` command in Router OSPF Configuration mode to enable OSPF 1583 compatibility. Use the `no` form of the command to disable it.

**Syntax**

```plaintext
compatible rfc1583
no compatible rfc1583
```

**Syntax Description**

This command has no arguments or keywords.

**Default Configuration**

Compatible with RFC 1583.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

**Example**

The following example enables 1583 compatibility.

```
console(config-router)#compatible rfc1583
```

**default-information originate (Router OSPF Configuration)**

Use the `default-information originate` command in Router OSPF Configuration mode to control the advertisement of default routes. Use the `no` form of the command to return the default route advertisement settings to the default value.
**Syntax**

default-information originate [always] [metric metric-value] [metric-type type-value]

no default-information originate [metric] [metric-type]

- **always**—Always advertise default routes.
- **metric-value**—The metric (or preference) value of the default route. (Range: 1–16777214)
- **type-value**—One of the following:
  1. External type-1 route.
  2. External type-2 route.

**Default Configuration**
The default configuration is `no default-information originate`. The default metric is none and the default type is 2.

**Command Mode**
Router OSPF Configuration mode.

**User Guidelines**
The only routers that actually have Internet connectivity should advertise a default route. All other routers in the network should learn the default route from the routers that have connections to the Internet. The edge router should also have a static default route configured with an upstream ISP router as the destination. The `always` keyword will cause the router to advertise a default route to its neighbors, even if no valid default route is known.

**Example**
The following example always advertises default routes.

```console
console(config-router)#default-information originate always metric 100 metric-type 1
```
default-metric

Use the default-metric command in Router OSPF Configuration mode to set a default for the metric of distributed routes. Use the no form of the command to remove the metric from the distributed routes. If the area has not been previously created, it is created by this command. If the area already exists, the default-metric information is added or modified.

Syntax

default-metric metric-value

no default-metric

- metric-value — The metric (or preference) value of the default route.
  (Range: 1–16777214)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets a value of 50 for the default metric.

```
console(config-router)#default-metric 50
```

distance ospf

The distance ospf command sets the preference values of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, external. All the external type routes are given the same preference value. Use the no form of this command to reset the preference values to the default.
Syntax

distance ospf {[intra-area dist1] [inter-area dist2] [external dist3]}

no distance ospf {intra-area | inter-area | external}

- intra-area dist1—Used to select the best path within an area when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).
- inter-area dist2—Used to select the best path from one area to another area when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).
- external dist3—Used to select the best path for routes from other routing domains, learned by redistribution when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).

Default Configuration

The default preference value is 110 for dist1, dist2 and dist3.

Command Mode

Router OSPF Configuration mode.

Router OSPFv3 Configuration mode.

User Guidelines

There are no user guidelines for this command.

Examples

The following examples set route preference values of OSPF in the router.

console(config-router)#distance ospf intra 4
console(config-router)#distance ospf type1 19

distribute-list out

Use the **distribute-list out** command in Router OSPF Configuration mode to specify the access list to filter routes received from the source protocol. Use the **no** form of the command to remove the specified source protocol from the access list.
Syntax

distribute-list name out {bgp | rip | static \ connected}

no distribute-list name out {bgp | rip | static \ connected}

• name—The name used to identify an existing ACL. The range is 1–31 characters.
• bgp—Apply the specified access list when BGP is the source protocol.
• rip—Apply the specified access list when RIP is the source protocol.
• static—Apply the specified access list when packets come through the static route.
• connected—Apply the specified access list when packets come from a directly connected route.

Default Configuration
This command has no default configuration.

Command Mode
Router OSPF Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example specifies the access list to filter routes received from the RIP source protocol.

console(config-router)#distribute-list ACL40 out rip

enable

Use the enable command in Router OSPF Configuration mode to set the administrative mode of OSPF in the router (active). OSPF is now globally enabled using the router ospf command. Use the no form of the command to disable the administrative mode for OSPF.
Syntax

enable
no enable

Default Configuration
Enabled is the default configuration.

Command Mode
Router OSPF Configuration mode.

User Guidelines
The no form of the enable command removes the OSPF router configuration from the running config. It does not, however, reset the OSPF configuration. For example, following no enable with the enable command restores the OSPF configuration to the running config.

OSPF must be disabled in order to assign or change the router ID.

Example
The following example enables OSPF router mode.

```
console(config-router)#enable
```

**exit-overflow-interval**
Use the exit-overflow-interval command in Router OSPF Configuration mode to configure the exit overflow interval for OSPF. When a router leaves the overflow state it can originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. Use the no form of the command to return the interval to the default value.

Syntax

exit-overflow-interval seconds
no exit-overflow-interval

- seconds — Number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. (Range: 0–2147483647)
Default Configuration
0 seconds is the default configuration.

Command Mode
Router OSPF Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets the exit overflow interval for OSPF at 10 seconds.
```
console(config-router)#exit-overflow-interval 10
```

external-lsdb-limit
Use the **external-lsdb-limit** command in Router OSPF Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. Use the no form of the command to return the limit to the default value.

Syntax
```
external-lsdb-limit integer
no external-lsdb-limit
```
- integer — Maximum number of non-default AS-external-LSAs allowed in the router's link-state database. (Range: –1 to 2147483647)

Default Configuration
-1 is the default configuration.

Command Mode
Router OSPF Configuration mode.
User Guidelines
The external LSDB limit MUST be set identically in all routers attached to
the OSPF backbone and/or any regular OSPF area.

Example
The following example configures the external LSDB limit for OSPF with the
number of non-default AS-external-LSAs set at 20.

```console
console(config-router)#external-lsdb-limit 20
```

**ip ospf area**
The `ip ospf area` command enables OSPFv2 and sets the area ID of an
interface. This command supersedes the effects of network area command. It
can also configure the advertisability of the secondary addresses on this
interface into OSPFv2 domain. Use the “no” form of this command to
disable OSPFv2 on an interface.

**Syntax**
- `ip ospf area area-id [secondaries none]`
- `no ip ospf area [secondaries none]`
  - `area-id` — The ID of the area (Range: IP address or decimal from 0 – 4294967295).

**Default Configuration**
OSPFv2 is disabled by default. No area id is configured by default.

**Command Mode**
Interface Configuration (VLAN) mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
```console
console(config-if-vlan1)#ip ospf area 192.168.1.10
console(config-if-vlan1)#ip ospf area 3232235786
```
**ip ospf authentication**

Use the `ip ospf authentication` command in the Interface Configuration mode to set the OSPF Authentication Type and Key for the specified interface. Use the no form of the command to return the authentication type to the default value.

**Syntax**

```
ip ospf authentication {none | {simple key} | {encrypt key key-id}}
```

```
no ip ospf authentication
```

- `encrypt` — MD5 encrypted authentication key.
- `key` — Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is `simple` and 16 bytes or less if the type is `encrypt`.)
- `key-id` — Authentication key identifier for the authentication type `encrypt`. (Range: 0–25)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

Unauthenticated interfaces do not need an authentication key or authentication key ID.

**Example**

The following example sets the OSPF Authentication Type and Key for VLAN 15.

```
console(config-if-vlan15)#ip ospf authentication encrypt test123 100
```
**ip ospf cost**

Use the `ip ospf cost` command in Interface Configuration mode to configure the cost on an OSPF interface. Use the `no` form of the command to return the cost to the default value.

**Syntax**

```
ip ospf cost interface-cost
no ip ospf cost
```

- `interface-cost` — Specifies the cost (link-state metric) of the OSPF interface. (Range: 1–65535)

**Default Configuration**

10 is the default link-state metric configuration.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures the cost on the OSPF interface at 5.

```
cfg-if-vlan1)#ip ospf cost 5
```

---

**ip ospf database-filter all out**

Use the `ip ospf database-filter all out` command in Interface Configuration mode to prevent flooding of OSPF LSAs on an interface. Use the `no` form of the command to enable flooding of LSAs on an interface.

**Syntax**

```
ip ospf database-filter all out
no ip ospf database-filter all out
```
**Default Configuration**
By default, LSAs are flooded on all interfaces in a routed VLAN.

**Command Mode**
Interface Configuration mode

**User Guidelines**
This command is only applicable to OSPFv2 routing configurations.

**ip ospf dead-interval**
Use the `ip ospf dead-interval` command in Interface Configuration to set the OSPF dead interval for the specified interface. Use the no form of the command to return the interval to the default value.

**Syntax**

\[
\text{ip ospf dead-interval seconds}
\]

\[
\text{no ip ospf dead-interval}
\]

- \( \text{seconds} \) — Number of seconds that a router’s Hello packets have not been seen before its neighbor routers declare that the router is down. (Range: \( 1–65535 \))

**Default Configuration**
40 is the default number of seconds.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e., 4).

**Example**
The following example sets the dead interval at 30 seconds.
ip ospf hello-interval

Use the ip ospf hello-interval command in Interface Configuration mode to set the OSPF hello interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

ip ospf hello-interval seconds
no ip ospf hello-interval

- seconds — Number of seconds to wait before sending Hello packets from the interface. (Range: 1–65535)

Default Configuration

10 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

The value for the length of time must be the same for all routers attached to a network.

Example

The following example sets the OSPF hello interval at 30 seconds.

console(config-if-vlan1)#ip ospf hello-interval 30

ip ospf mtu-ignore

Use the ip ospf mtu-ignore command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the
Database Description packet is rejected and the OSPF adjacency is not established. Use the no form of the command to enable OSPF maximum transmission unit (MTU) mismatch detection.

**Syntax**

ip ospf mtu-ignore
no ip ospf mtu-ignore

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example disables OSPF MTU mismatch detection on VLAN interface 15.

```
console(config-if-vlan1)#ip ospf mtu-ignore
```

**ip ospf network**

Use the `ip ospf network` command to configure OSPF to treat an interface as a point-to-point rather than broadcast interface. To return to the default value, use the no form of this command.

**Syntax**

```
ip ospf network {broadcast | point-to-point}
no ip ospf network
```

- broadcast — Set the network type to broadcast.
- point-to-point — Set the network type to point-to-point
Default Configuration
Interfaces operate in broadcast mode by default.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
OSPF treats interfaces as broadcast interfaces by default. Loopback interfaces have a special loopback network type, which cannot be changed. When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Example
The following example shows the options for the ip ospf network command.

crash (config-if-vlan1)#ip ospf network ?

broadcast Set the OSPF network type to Broadcast
point-to-point Set the OSPF network type to Point-to-Point

ip ospf priority
Use the ip ospf priority command in Interface Configuration mode to set the OSPF priority for the specified router interface. Use the no form of the command to return the priority to the default value.

Syntax
ip ospf priority number-value
no ip ospf priority

- number-value — Specifies the OSPF priority for the specified router interface. (Range: 0–255)

Default Configuration
1 is the default integer value.
**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.

**Example**

The following example sets the OSPF priority for the VLAN 15 router at 100.

```
console(config-if-vlan1)#ip ospf priority 100
```

**ip ospf retransmit-interval**

Use the `ip ospf retransmit-interval` command in Interface Configuration mode to set the OSPF retransmit Interval for the specified interface. Use the no form of the command to return the interval to the default value.

**Syntax**

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

- seconds — Number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0–3600 seconds)

**Default Configuration**

5 is the default number of seconds.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.
Example
The following example sets the OSPF retransmit Interval for VLAN 15 at 50 seconds.

```
console(config-if-vlan1)#ip ospf retransmit-interval 50
```

**ip ospf transmit-delay**
Use the `ip ospf transmit-delay` command in Interface Configuration mode to set the OSPF Transit Delay for the specified interface. Use the no form of the command to return the delay to the default value.

**Syntax**
```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```
- `seconds` — Sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1–3600 seconds)

**Default Configuration**
1 is the default number of seconds.

**Command Mode**
Interface Configuration (VLAN) mode.

**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets the OSPF Transit Delay for VLAN 15 at 20 seconds.

```
console(config-if-vlan1)#ip ospf transmit-delay 20
```

**log adjacency-changes**
Use the `log adjacency-changes` command in OSPFv2 Router Configuration mode to enable logging of OSPFv2 neighbor state changes.
Use the `no` form of the command to disable state change logging.

**Syntax**

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

- `detail`—(Optional) When this keyword is specified, all adjacency state changes are logged. Otherwise, OSPF only logs transitions to FULL state and when a backwards transition occurs.

**Default Configuration**

Adjacency changes are not logged by default.

**Command Mode**

OSPFv2 Router Configuration mode

**User Guidelines**

State changes are logged with INFORMATIONAL severity.

**max-metric router-lsa**

Use the `max-metric router-lsa` command in router OSPF Global Configuration mode to configure OSPF to enable stub router mode.

To disable stub router mode, use the `no max-metric router-lsa` command in OSPFv2 Global Router Configuration mode.

**Syntax**

max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]

no max-metric router-lsa [on-startup] [summary-lsa]

- `on-startup`—(Optional) OSPF starts in stub router mode after a reboot.
- `seconds`—(Required if on-startup) The number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
- `summary-lsa`—(Optional) Set the metric in type 3 and 4 summary LSAs to LsInfinity (0xffffffff).
metric—(Optional) Metric to send in summary LSAs when in stub router mode. Range is 1 to 16,777,215. Default is 16,711,680 (0xFF0000).

Default Configuration
By default, OSPF is not in stub router mode.

Command Mode
OSPFv2 Global Configuration mode

User Guidelines
When OSPF is in stub router mode, as defined by RFC 3137, OSPF sets the metric in the non-stub links in its router LSA to LsInfinity. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

One can administratively force OSPF into stub router mode. OSPF remains in stub router mode until OSPF is taken out of stub router mode. Alternatively, one can configure OSPF to start in stub router mode for a specific period of time after the router boots up.

If the summary LSA metric is set to 16,777,215, other routers will skip the summary LSA when they compute routes.

If the router is configured to enter stub router mode on startup (max-metric router-lsa on-startup), and one then enters max-metric router lsa, there is no change. If OSPF is administratively in stub router mode (the max-metric router-lsa command has been given), and one configures OSPF to enter stub router mode on startup (max-metric router-lsa on-startup), OSPF exits stub router mode (assuming the startup period has expired) and the configuration is updated.

The command no max-metric router-lsa clears either type of stub router mode (always or on-startup) and resets the summary-lsa option. If OSPF is configured to enter global configuration mode on startup, and during normal operation one wants to immediately place OSPF in stub router mode, one
may issue the command no max-metric router-lsa on-startup. The command no max-metric router-lsa summary-lsa causes OSPF to send summary LSAs with metrics computed using normal procedures defined in RFC 2328.

**maximum-paths**

Use the `maximum-paths` command in Router OSPF Configuration mode to set the number of paths that OSPF can report for a given destination. Use the no form of the command to reset the number to the default value.

**Syntax**

```
maximum-paths integer
no maximum-paths
```

- `integer` — Number of paths that OSPF can report for a given destination. (Range: 1–4.)

**Default Configuration**

4 is the integer default value.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

OSPF is only enabled on an interface if the primary IPv4 address on the interface matches a network area range. Any individual interface can only be attached to a single area. If an interface address matches multiple network area ranges, the interface is assigned to the area for the first matching range. If the `ip ospf area` command is given for an interface, it overrides any matching network area command.

OSPF only advertises IP subnets for secondary IP addresses if the secondary address is within the range of a network area command for the same area as the primary address on the same interface.

When a network area command is deleted, matching interfaces are reevaluated against all remaining network area commands.
Example
The following example sets the number of paths at 2 that OSPF can report for a given destination.

```console
console(config-router)#maximum-paths 2
```

**network area**

The **network area** command enables OSPFv2 on an interface and sets its area ID if the ip-address of an interface is covered by this network command. Use the “no” form of this command to disable OSPFv2 on an interface.

**Syntax**

```markdown
network ip-address wildcard-mask area area-id
no network ip-address wildcard-mask area area-id
```

- ip-address — Base IPv4 address of the network area.
- wildcard-mask — The network mask indicating the wildcard bit. A 1 bit in the mask indicates a don’t care condition for the corresponding bit in the address.
- area-id — The ID of the area (Range: IPv4 address or 32-bit decimal in the range 0–4294967295).

**Default Configuration**

OSPFv2 is disabled

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

OSPF is only enabled on an interface if the primary IPv4 address on the interface matches a network area range. Any individual interface can only be attached to a single area. If an interface address matches multiple network area ranges, the interface is assigned to the area for the first matching range. If the **ip ospf area** command is given for an interface, it overrides any matching network area command.
OSPF only advertises IP subnets for secondary IP addresses if the secondary address is within the range of a network area command for the same area as the primary address on the same interface.

When a network area command is deleted, matching interfaces are reevaluated against all remaining network area commands. Ones in the wildcard mask indicate “don’t care” bits in the network address.

Example

```
console(config-router)#network 10.50.50.0 0.0.0.255 area 4
```

**nsf**

Use this command to enable OSPF graceful restart. Use the no form of this command to disable graceful restart.

**Syntax**

```
nsf [ietf] [planned-only]
```

```
no nsf [ietf]
```

- **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

- **planned-only** — This keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

**Default Configuration**

Graceful restart is disabled by default

**Command Mode**

Router OSPF Configuration mode

**User Guidelines**

Graceful restart works in concert with nonstop forwarding to enable the hardware to continue forwarding IPv4 packets using OSPFv2 routes while a backup unit takes over management unit responsibility. When OSPF
executes a graceful restart, it informs its neighbors that the OSPF control plane is restarting, but that it will be back shortly. Helpful neighbors continue to advertise to the rest of the network that they have full adjacencies with the restarting router, avoiding announcement of a topology change and everything that goes with that (i.e., flooding of LSAs, SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors. This implementation of graceful restart restarting router behavior is only useful with a router stack. Graceful restart does not work on a standalone, single-unit router.

**nsf helper**

Use the `nsf-helper` to allow OSPF to act as a helpful neighbor for a restarting router. Use the “no” form of this command to prevent OSPF from acting as a helpful neighbor.

**Syntax**

```
nsf [ietf] helper[planned-only]
no nsf [ietf] helper
```

- `planned-only` — This keyword indicates that OSPF should only help a restarting router performing a planned restart.

**Default Configuration**

OSPF may act as a helpful neighbor for both planned and unplanned restarts

**Command Mode**

Router OSPF Configuration mode

**User Guidelines**

The grace LSA announcing the graceful restart includes a restart reason. Reasons 1 (software restart) and 2 (software reload/upgrade) are considered planned restarts. Reasons 0 (unknown) and 3 (switch to redundant control processor) are considered unplanned restarts.

`nsf ietf helper disable` is functionally equivalent to no nsf helper and is supported solely for IS CLI compatibility.
nsf helper strict-lsa-checking

Use the `nsf-helper strict-lsa-checking` command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the “no” form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Syntax

`nsf [ietf] helper strict-lsa-checking`

`no nsf [ietf] helper strict-lsa-checking`

- `ietf` — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

Default Configuration

A helpful neighbor exits helper mode when a topology change occurs.

Command Mode

Router OSPF Configuration mode

User Guidelines

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router.

A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

nsf restart-interval

Use the `nsf restart-interval` command to configure the length of the grace period on the restarting router. Use the “no” form of this command to revert the grace period to its default.
Syntax
nsf [ietf] restart-interval seconds
no nsf [ietf] restart-interval

- ietf — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.
- seconds — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1–1800 seconds).

Default Configuration
The default restart interval is 120 seconds.

Command Mode
Router OSPF

User Guidelines
The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Example
console(config-router)#nsf restart-interval 180

passive-interface default
The passive-interface default command enables the global passive mode by default for all interfaces. It overrides any interface level passive mode. Use the “no” form of this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Syntax
passive-interface default
no passive-interface default
**Default Configuration**
Global passive mode is disabled by default.

**Command Mode**
Router OSPF Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
corsole(config-router)#passive-interface

coresole(config-router)#passive-interface

**passive-interface**
Use the `passive-interface` command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface. Use the “no” form of this command to set the interface as non-passive.

**Syntax**

```plaintext
passive-interface vlan vlan-id
no passive-interface vlan vlan-id
```

- `vlan-id` — The VLAN number

**Default Configuration**
Passive interface mode is disabled by default.

**Command Mode**
Router OSPF Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
coresole(config-router)#passive-interface vlan 1
**redistribute (OSPF)**

Use the `redistribute` command in Router OSPF Configuration mode to configure OSPF protocol to allow redistribution of routes from the specified source protocol/routers. Use the `no` version of the command to disable redistribution from the selected source or to reset options to their default values.

**Syntax**

```
redistribute {protocol} [metric metric-value] [metric-type type-value] [tag tag-value] [subnets]

no redistribute {protocol} [metric] [metric-type] [tag] [subnets]
```

- **protocol** — One of the following:
  - static—Specifies that static routes are to be redistributed.
  - connected—Specifies that connected routes are to be redistributed.
  - bgp—Specifies BGP originated routes are to be redistributed.
  - rip—Specifies RIP originated routes are to be redistributed.
- **metric-value** — Specifies the metric to use when redistributing the route. (Range: 0–16777214)
- **type-value** — One of the following:
  - Type 1 external route.
  - Type 2 external route.
- **tag-value** — Inserts the specified tag value into redistributed routes. (Range: 0–4294967295)
- **subnets** — Specifies whether to redistribute the routes to subnets.

**Default Configuration**

The default tag value is 0.

There is no default metric or route map configured.

**Command Mode**

Router OSPF Configuration mode
User Guidelines

When redistributing a route metric, the receiving protocol must understand the metric. The OSPF metric is a cost value equal to $10^8$/ link bandwidth in bits/sec. For example, the OSPF cost of GigabitEthernet is $10^8/10^8 = 1$.

The RIP metric is a hop count with a maximum value of 15 (infinity).

If no metric value is specified, the metric redistributed for a type 1 route is the sum of the external cost and the internal cost used to reach that route.

The metric redistributed for a type 2 route is always the external cost, irrespective of the interior cost to reach that route. Redistribution of BGP originated routes is only available on BGP-capable routers.

Example

The following example configures OSPF protocol to allow redistribution of RIP originated routes with a metric of 5 and a route tag of 555.

```
console(config-router)#redistribute rip metric 3 metric-type 1 tag 555
```

router-id

Use the `router-id` command in Router OSPF Configuration mode to set a 32-bit integer in 4-digit dotted-decimal number uniquely identifying the router ID.

Syntax

```
router-id router-id
```

- `router-id`— A 32-bit interface (in IPv4 address format) that uniquely identifies the router ID.

Default Configuration

There is no default router ID.

Command Mode

Router OSPF Configuration mode.
User Guidelines
The router-id must be set in order for OSPF to become operationally enabled. It is recommended that the router ID be set to the IP address of a loopback interface to ensure that the router remains up internally.

Example
The following example defines the router ID as 5.5.5.5.

```
console(config)#router ospf
console(config-router)#router-id 5.5.5.5
```

router ospf
Use the `router ospf` command in Global Configuration mode to enter Router OSPF mode and globally enable OSPF. Using the no form of the command disables OSPF and removes the OSPF interface and global configuration.

Syntax
```
router ospf [vrf vrf-name]
no router ospf
```

- `vrf-name`—The name of the VRF if which OSPF is to be enabled. If no VRF is specified, OSPF is enabled for the global routing instance.

Default Configuration
OSPF routing is disabled by default

Command Mode
Global Configuration mode.

User Guidelines
The command prompt changes when the `router ospf` command executes. The VRF identified in the parameter must have been previously created or an error is returned. This command is only available on the N3000/N3100/N4000 switches. IPv4 OSPF is the only routing protocol currently implemented for VRFs.
The no form of the command removes all OSPF configuration (including interface configuration) for the specified VRF.

**Example**
The following example enters into router OSPF mode.

```
console(config)#router ospf
console(config-router)#
```

**show ip ospf**
Use the `show ip ospf` command to display information relevant to the OSPF router. This command has been modified to show additional fields.

**Syntax**
```
show ip ospf [vrf vrf-name]
```
- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Syntax Description**
This command has no arguments or keywords.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**
The VRF identified in the parameter must have been previously created or an error is returned.
The VRF parameter is only available on the N3000/N3100/N4000 series switches.
Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Shows whether OSPF is administratively enabled or disabled.</td>
</tr>
<tr>
<td>RFC 1583 Compatibility</td>
<td>This configuration option controls the preference rules used when choosing among multiple external LSAs advertising the same destination. When enabled, the preference rules remain those specified by RFC 1583. When disabled, the preference rules are those stated in Section 16.4.1 of RFC 2328. These rules prevent routing loops when external LSAs for the same destination have been originated from different areas.</td>
</tr>
<tr>
<td>External LSDB Limit</td>
<td>Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.</td>
</tr>
<tr>
<td>Exit Overflow Interval</td>
<td>Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.</td>
</tr>
<tr>
<td>Spf Delay Time</td>
<td>The number of seconds to wait before running a routing table calculation after a topology change.</td>
</tr>
<tr>
<td>Spf Hold Time</td>
<td>The minimum number of seconds between routing table calculations.</td>
</tr>
<tr>
<td>Flood Pacing Interval</td>
<td>The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the <code>timers pacing flood</code> command.</td>
</tr>
<tr>
<td>LSA Refresh Group Pacing Time</td>
<td>The size of the LSA refresh group window, in seconds. This is the value configured with the <code>timers pacing lsa-group</code> command.</td>
</tr>
<tr>
<td>Opaque Capability</td>
<td>Shows whether router is capable of sending Opaque LSAs.</td>
</tr>
<tr>
<td>AutoCost Ref BW</td>
<td>The configured autocost reference bandwidth. This value is used to determine the OSPF metric on its interfaces. The reference bandwidth is divided by the interface speed to compute the metric.</td>
</tr>
<tr>
<td><strong>Default Passive Setting</strong></td>
<td>When enabled, OSPF interfaces are passive by default.</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td><strong>Maximum Paths</strong></td>
<td>Shows the maximum number of paths that OSPF can report for a given destination.</td>
</tr>
<tr>
<td><strong>Default Metric</strong></td>
<td>Default metric for redistributed routes.</td>
</tr>
<tr>
<td><strong>Stub Router Configuration</strong></td>
<td>One of Always, Startup, or None.</td>
</tr>
<tr>
<td><strong>Stub Router Startup Time</strong></td>
<td>Configured value in seconds. This row is only listed if OSPF is configured to be a stub router at startup.</td>
</tr>
<tr>
<td><strong>Summary LSA Metric Override</strong></td>
<td>One of Enabled (met), Disabled, where met is the metric to be sent in summary LSAs when in stub router mode.</td>
</tr>
<tr>
<td><strong>BFD Enabled</strong></td>
<td>The BFD status.</td>
</tr>
<tr>
<td><strong>Default Route Advertise</strong></td>
<td>When enabled, OSPF originates a type 5 LSA advertising a default route.</td>
</tr>
<tr>
<td><strong>Always</strong></td>
<td>When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.</td>
</tr>
<tr>
<td><strong>Metric Type</strong></td>
<td>Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.</td>
</tr>
<tr>
<td><strong>Number of Active Areas</strong></td>
<td>The number of OSPF areas to which the router is attached on interfaces that are up.</td>
</tr>
<tr>
<td><strong>ABR Status</strong></td>
<td>Shows whether the router is an OSPF Area Border Router.</td>
</tr>
<tr>
<td><strong>ASBR Status</strong></td>
<td>Indicates whether the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from another protocol. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).</td>
</tr>
<tr>
<td><strong>Stub Router Status</strong></td>
<td>One of Active or Active.</td>
</tr>
<tr>
<td><strong>Stub Router Reason</strong></td>
<td>One of Configured, Startup, or Resource Limitation. This row is only listed if stub router is active.</td>
</tr>
<tr>
<td><strong>Layer 3 Routing Commands</strong></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Layer 3 Routing Commands</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stub Router Time Remaining</strong></td>
<td>The remaining time until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode.</td>
</tr>
<tr>
<td><strong>External LSDB Overflow</strong></td>
<td>OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.</td>
</tr>
<tr>
<td><strong>External LSA Count</strong></td>
<td>Shows the number of external (LS type 5) link-state advertisements in the link-state database.</td>
</tr>
<tr>
<td><strong>External LSA Checksum</strong></td>
<td>Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.</td>
</tr>
<tr>
<td><strong>AS_OPAQUE LSA Count</strong></td>
<td>Shows the number of AS Opaque LSAs received.</td>
</tr>
<tr>
<td><strong>AS_OPAQUE LSA Checksum</strong></td>
<td>Sum of the checksums of all AS Opaque LSAs in the link state database.</td>
</tr>
<tr>
<td><strong>New LSAs Originated</strong></td>
<td>Shows the number of link-state advertisements that have been originated.</td>
</tr>
<tr>
<td><strong>LSAs Received</strong></td>
<td>Shows the number of link-state advertisements received determined to be new instantiations.</td>
</tr>
<tr>
<td><strong>LSA Count</strong></td>
<td>The number of LSAs in the link state database.</td>
</tr>
<tr>
<td><strong>Maximum Number of LSAs</strong></td>
<td>The limit on the number of LSAs that the router can store in its link state database.</td>
</tr>
<tr>
<td><strong>LSA High Water Mark</strong></td>
<td>The maximum number of LSAs that have been in the link state database since OSPF began operation.</td>
</tr>
<tr>
<td><strong>AS Scope LSA Flood List Length</strong></td>
<td>The number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain. LSAs with AS flooding scope, such as type 5 external LSAs and type 11 Opaque LSAs.</td>
</tr>
<tr>
<td><strong>Retransmit List Entries</strong></td>
<td>The current number of entries on all neighbors’ retransmit lists.</td>
</tr>
<tr>
<td><strong>Maximum Number of Retransmit Entries</strong></td>
<td>The maximum number of entries that can be on neighbors’ retransmit lists at any given time. This is the sum for all neighbors. When OSPF receives an LSA and cannot allocate a new retransmit list entry, the router does not acknowledge the LSA, expecting the sender to retransmit.</td>
</tr>
<tr>
<td><strong>Retransmit Entries High Water Mark</strong></td>
<td>The maximum number of retransmit list entries that have been on all neighbors’ retransmit lists at one time.</td>
</tr>
<tr>
<td><strong>NSF Support</strong></td>
<td>Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.</td>
</tr>
<tr>
<td>NSF Restart Interval</td>
<td>The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NSF Restart Status</td>
<td>Whether the router is currently performing a graceful restart.</td>
</tr>
<tr>
<td>NSF Restart Age</td>
<td>The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.</td>
</tr>
<tr>
<td>NSF Restart Exit Reason</td>
<td>The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.</td>
</tr>
<tr>
<td>NSF Helper Support</td>
<td>Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.</td>
</tr>
<tr>
<td>NSF Helper Strict LSA Checking</td>
<td>As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.</td>
</tr>
<tr>
<td>Redistributing</td>
<td>This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.</td>
</tr>
<tr>
<td>Source</td>
<td>Shows source protocol/routes that are being redistributed. Possible values are BGP, connected, RIP, and static.</td>
</tr>
<tr>
<td>Tag</td>
<td>Shows the decimal value attached to each external route.</td>
</tr>
<tr>
<td>Subnets</td>
<td>When this option is not configured, OSPF will only redistribute classful prefixes.</td>
</tr>
<tr>
<td>Distribute-List</td>
<td>Shows the access list used to filter redistributed routes.</td>
</tr>
</tbody>
</table>

**Example #1**

The following example displays OSPF router information.

```
console#show ip ospf
```

- **Router ID**: 1.1.1.1
- **OSPF Admin Mode**: Enable
- **RFC 1583 Compatibility**: Enable
- **External LSDB Limit**: No Limit
- **Exit Overflow Interval**: 0
- **Spf Delay Time**: 5
- **Spf Hold Time**: 10
- **Opaque Capability**: Disable
- **AutoCost Ref BW**: 100 Mbps
- **Default Passive Setting**: Disabled
Maximum Paths............................ 4
Default Metric........................... Not configured
Default Metric........................... Not configured
Stub Router Configuration.............. None
Summary LSA Metric Override.......... Disabled

BFD Enabled............................. NO

Default Route Advertise............... Disabled
Always.................................. FALSE
Metric.................................. Not configured
Metric Type............................ External Type 2

Number of Active Areas... 1 (1 normal, 0 stub, 0 nssa)
ABR Status.............................. Disable
ASBR Status............................. Disable
Stub Router.............................. FALSE
External LSDB Overflow............... FALSE
External LSA Count..................... 0
External LSA Checksum................ 0
AS_OPAQUE LSA Count.................. 0
AS_OPAQUE LSA Checksum.............. 0
New LSAs Originated................... 25
LSAs Received......................... 7
LSA Count.............................. 4
Maximum Number of LSAs.............. 18200
LSA High Water Mark.................. 4
Retransmit List Entries............... 0
Maximum Number of Retransmit Entries 72800
Retransmit Entries High Water Mark... 2

NSF Support............................ Disabled
NSF Restart Interval................... 120
NSF Restart Status..................... Not Restarting
NSF Restart Age........................ 0 seconds
NSF Restart Exit Reason.............. Not Attempted
NSF Helper Support..................... Always
NSF Helper Strict LSA Checking...... Enabled

Example #2

The following example displays the length of the global flood queue for LSAs with AS flooding scope and for stub router configuration. Also displayed are the values of the LSA pacing configuration parameters.

console#show ip ospf
Router ID...................................... 1.1.1.1
OSPF Admin Mode.......................... Enable
RFC 1583 Compatibility.................. Enable
External LSDB Limit...................... No Limit
Exit Overflow Interval......................... 0
Spf Delay Time.................................. 5
Spf Hold Time................................. 10
Flood Pacing Interval......................... 33 ms
LSA Refresh Group Pacing Time.............. 60 sec
Opaque Capability.............................. Enable
AutoCost Ref BW................................ 100 Mbps
Default Passive Setting........................ Disabled
Maximum Paths.................................. 4
Default Metric.................................. Not configured
Stub Router Configuration..................... <val>
Stub Router Startup Time...................... <val> seconds
Summary LSA Metric Override................... Enabled (<met>)
BFD Enabled.................................... YES

Default Route Advertise........................ Disabled
Always......................................... FALSE
Metric......................................... Not configured
Metric Type.................................... External Type 2

Number of Active Areas......................... 2 (2 normal, 0 stub, 0 nssa)
ABR Status...................................... Enable
ASBR Status..................................... Disable
Stub Router Status............................. Inactive
Stub Router Reason............................. <reason>
Stub Router Time Remaining.................... <duration> seconds
External LSDB Overflow....................... FALSE
External LSA Count............................ 0
External LSA Checksum.......................... 0
AS_OPAQUE LSA Count........................... 0
AS_OPAQUE LSA Checksum....................... 0
New LSAs Originated........................... 300269
LSAs Received................................. 300276
LSA Count...................................... 6020
Maximum Number of LSAs...................... 36968
LSA High Water Mark........................... 6020
AS Scope LSA Flood List Length.............. 0
Retransmit List Entries....................... 0
Maximum Number of Retransmit Entries........ 147872
Retransmit Entries High Water Mark......... 32616
NSF Helper Support............................ Always
NSF Helper Strict LSA Checking............... Enabled

**show ip ospf abr**

The `show ip ospf abr` command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.
Syntax

show ip ospf abr [vrf vrf-name]

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

Example

```
console#show ip ospf abr
Type  Router Id   Cost  Area ID         Next Hop    Next Hop Intf
----- ---------   ----- --------------- ---------   --------
INTRA 3.3.3.3     1     0.0.0.1         10.1.23.3   vlan11
INTRA 4.4.4.4     10    0.0.0.1         10.1.24.4   vlan12
```

**show ip ospf area**

Use the `show ip ospf area` command to display information about the identified OSPF area.

Syntax

show ip ospf area area-id [vrf vrf-name]

- area-id—Identifies the OSPF area whose ranges are being displayed. (Range: 0–4294967295)
• vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example #1**

The following example displays OSPF router information.

```
console#show ip ospf area 10
AreaID......................................... 0.0.0.10
External Routing............................... Import External LSAs
Spf Runs....................................... 0
Area Border Router Count....................... 0
Area LSA Count................................. 0
Area LSA Checksum.............................. 0
Import Summary LSAs............................ Enable
```

**Example #2**

```
console#show ip ospf area 20
AreaID......................................... 0.0.0.20
External Routing............................... Import NSSAs
Spf Runs....................................... 0
Area Border Router Count....................... 0
Area LSA Count................................. 0
Area LSA Checksum.............................. 0
OSPF NSSA Specific Information.
Import Summary LSAs............................ Enable
Redistribute into NSSA.......................... Enable
Default Information Originate.................. TRUE
Default Metric................................ 250
Default Metric Type............................ Non-Comparable
```
Translator Role................................ Candidate
Translator Stability Interval.................. 2000
Translator State............................... Disabled

Example #3
The following example shows the length of the area’s flood queue for LSAs waiting to be flooded within the area.

console #show ip ospf area 1

AreaID......................................... 0.0.0.1
External Routing............................... Import External LSAs
Spf Runs....................................... 10
Area Border Router Count....................... 0
Area LSA Count................................. 3004
Area LSA Checksum.............................. 0x5e0abed
Flood List Length.............................. 0
Import Summary LSAs............................ Enable

show ip ospf asbr
The show ip ospf asbr command displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax
show ip ospf asbr [vrf vrf-name]

• vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

Example

```
close#show ip ospf asbr
```

<table>
<thead>
<tr>
<th>Type</th>
<th>Router Id</th>
<th>Cost</th>
<th>Area ID</th>
<th>Next Hop</th>
<th>Next Hop Intf</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRA</td>
<td>1.1.1.1</td>
<td>1</td>
<td>0.0.0.1</td>
<td>10.1.12.1</td>
<td>vlan10</td>
</tr>
<tr>
<td>INTRA</td>
<td>4.4.4.4</td>
<td>10</td>
<td>0.0.0.1</td>
<td>10.1.24.4</td>
<td>vlan12</td>
</tr>
</tbody>
</table>

show ip ospf database

Use the `show ip ospf database` command to display information about the link state database when OSPF is enabled. If parameters are entered, the command displays the LSA headers. Use the optional parameters to specify the type of link state advertisements to display.

Syntax

```
show ip ospf [vrf vrf-name] [area-id] database [{asbr-summary | external | network | nssa-external | router | summary}] [ls-id] [adv-router [ip-address] | self-originate] [opaque-area] [opaque-as] [opaque-link]
```

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- area-id — Identifies a specific OSPF area for which link state database information will be displayed.
- asbr-summary — Display the autonomous system boundary router (ASBR) summary LSAs.
- external — Display the external LSAs.
- network — Display the network LSAs.
- nssa-external — Display NSSA external LSAs.
- router — Display router LSAs.
• summary — Display the LSA database summary information.
• ls-id — Specifies the link state ID (LSID). (Range: IP address or an integer in the range of 0–4294967295)
• adv-router — Display the LSAs that are restricted by the advertising router. To specify a router, enter the IP address of the router.
• self-originate — Display the LSAs in that are self-originated.
• opaque-area — Display the area opaque LSAs.
• opaque-as — Display AS opaque LSAs.
• opaque-link — Display link opaque LSAs.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
Information is only displayed if OSPF is enabled.
The VRF identified in the parameter must have been previously created or an error is returned.
The VRF parameter is only available on the N3000/N3100/N4000 series switches.

Example
The following example displays information about the link state database when OSPF is enabled.

```
console#show ip ospf database

Router Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksum</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1360</td>
<td>80000006</td>
<td>3a1f</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>5.2.0.0</td>
<td>5.2.0.0</td>
<td>1360</td>
<td>80000009</td>
<td>a47e</td>
<td>--------</td>
<td>---E---</td>
</tr>
<tr>
<td>20.20.20.20</td>
<td>20.20.20.20</td>
<td>1165</td>
<td>8000000b</td>
<td>0f80</td>
<td>-E-----</td>
<td>--------</td>
</tr>
</tbody>
</table>
```
### Network Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>20.20.20.20</td>
<td>1165</td>
<td>80000005</td>
<td>f86d</td>
<td>-E--O--</td>
<td></td>
</tr>
</tbody>
</table>

### Network Summary States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1360</td>
<td>80000007</td>
<td>242e</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

### Summary ASBR States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1361</td>
<td>80000006</td>
<td>183a</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

### Link Opaque States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1361</td>
<td>80000005</td>
<td>ef59</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

### Area Opaque States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1362</td>
<td>80000005</td>
<td>e166</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

### AS External States

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0.0</td>
<td>5.2.0.0</td>
<td>1364</td>
<td>80000008</td>
<td>e35d</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

### AS Opaque States

<table>
<thead>
<tr>
<th>Link Id</th>
<th>Adv Router</th>
<th>Age</th>
<th>Sequence</th>
<th>Chksm</th>
<th>Options</th>
<th>Rtr Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0.0</td>
<td>0.0.0.0</td>
<td>1364</td>
<td>80000005</td>
<td>d373</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>
**show ip ospf database database-summary**

Use the **show ip ospf database database-summary** command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database. This command has been modified.

**Syntax**

```plaintext
show ip ospf database database-summary [vrf vrf-name]
```

- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Shows Total number of router LSAs in the OSPF link state database.</td>
</tr>
<tr>
<td>Network</td>
<td>Shows Total number of network LSAs in the OSPF link state database.</td>
</tr>
<tr>
<td>Summary Net</td>
<td>Shows Total number of summary network LSAs in the database.</td>
</tr>
</tbody>
</table>
The following example displays the number of each type of LSA in the database for each area and for the router.

```
console#show ip ospf database database-summary
OSPF Router with ID (5.5.5.5)
Area 0.0.0.0 database summary
  Router......................................... 0
  Network........................................ 0
  Summary Net.................................... 0
  Summary ASBR................................... 0
  Type-7 Ext..................................... 0
  Self Originated Type-7......................... 0
  Opaque Link.................................... 0
  Opaque Area.................................... 0
  Subtotal....................................... 0
Area 0.0.0.10 database summary
  Router......................................... 0
  Network........................................ 0
  Summary Net.................................... 0
  Summary ASBR................................... 0
  Type-7 Ext..................................... 0
  Self Originated Type-7......................... 0
  Opaque Link.................................... 0
  Opaque Area.................................... 0
  Subtotal....................................... 0
Router database summary
  Router......................................... 0
  Network........................................ 0
  Summary Net.................................... 0
  Summary ASBR................................... 0
```

| Summary ASBR | Shows Number of summary ASBR LSAs in the database. |
| Type-7 Ext | Shows Total number of Type-7 external LSAs in the database. |
| Self-Originated Type-7 | Shows Total number of self originated AS external LSAs in the OSPFv3 link state database. |
| Opaque Link | Shows Number of opaque link LSAs in the database. |
| Opaque Area | Shows Number of opaque area LSAs in the database. |
| Subtotal | Shows Number of entries for the identified area. |
| Opaque AS | Shows Number of opaque AS LSAs in the database. |
| Total | Shows Number of entries for all areas. |
show ip ospf interface

Use the `show ip ospf interface` command to display the information for the VLAN or loopback interface. The long form of the command displays the configuration of flood blocking.

**Syntax**

```
show ip ospf interface [vrf vrf-name][vlan vlan-id | loopback loopback-id]
```

- `loopback-id`—A configured loopback interface identifier. (Range: 0-7)
- `vlan-id`—A configured VLAN identifier. (Range: 0-4093)
- `vrf-name`—The name of the VRF instance on which the command operates. If no vrf parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example #1**

The following example displays the information for the IFO object or virtual interface tables associated with VLAN 10.

```
console#show ip ospf interface vlan 10

IP Address..................................... 1.1.1.1
```
Subnet Mask.............................. 255.255.255.0
Secondary IP Address(es)..............
OSPF Admin Mode......................... Enable
OSPF Area ID............................. 0.0.0.0
OSPF Network Type....................... Broadcast
Router Priority.......................... 1
Retransmit Interval...................... 5
Hello Interval............................ 10
Dead Interval............................. 40
LSA Ack Interval........................ 1
Transmit Delay Interval................. 1
Authentication Type..................... None
Metric Cost................................ 10 (computed)
Passive Status............................ Non-passive interface
OSPF Mtu-ignore......................... Disable
State...................................... designated-router
Designated Router....................... 1.1.1.1
Backup Designated Router.............. 0.0.0.0
Number of Link Events............... 2

Example #2

The following example shows the configuration of flood blocking.

console#show ip ospf interface gi2/0/11

IP Address........................... 172.20.11.2
Subnet Mask.......................... 255.255.255.0
Secondary IP Address(es)..............
OSPF Admin Mode......................... Enable
OSPF Area ID............................. 0.0.0.0
OSPF Network Type....................... Point-to-Point
Router Priority.......................... 1
Retransmit Interval...................... 5
Hello Interval............................ 3
Dead Interval............................. 12
LSA Ack Interval........................ 1
Transmit Delay Interval................. 1
Authentication Type..................... None
Metric Cost................................ 100 (computed)
Passive Status............................ Non-passive interface
OSPF Mtu-ignore......................... Disable
Flood Blocking......................... Disable
State..................................... point-to-point
Number of Link Events............... 1
Local Link LSAs......................... 0
Local Link LSA Checksum............... 0
**show ip ospf interface brief**

Use the `show ip ospf interface brief` command to display brief information for the IFO object or virtual interface tables.

**Syntax**

`show ip ospf interface brief [vrf vrf-name]`

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example**

The following example displays brief information for the IFO object or virtual interface tables.

```
console#show ip ospf interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Area ID</th>
<th>Hello Int.</th>
<th>Dead Int.</th>
<th>Retrax Int.</th>
<th>Val.</th>
<th>Delay</th>
<th>Intval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vl10</td>
<td>Enable</td>
<td>0.0.0.10</td>
<td>1</td>
<td>10</td>
<td>40</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vl20</td>
<td>Enable</td>
<td>0.0.0.1</td>
<td>1</td>
<td>10</td>
<td>40</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vl100</td>
<td>Enable</td>
<td>0.0.0.111</td>
<td>1</td>
<td>10</td>
<td>40</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>loopback 1</td>
<td>Enable</td>
<td>0.0.0.0</td>
<td>1</td>
<td>1</td>
<td>40</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```
**show ip ospf interface stats**

Use the show ip ospf interface stats command to display the statistics for a specific interface. The information is only displayed if OSPF is enabled.

**Syntax**

```
show ip ospf interface stats vlan vlan-id
```

- **vlan-id** — Valid VLAN ID.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the ospf statistics for VLAN 15.

```
console>show ip ospf interface stats vlan 15
OSPF Area ID............................................... 0.0.0.0
Area Border Router Count................................. 0
AS Border Router Count................................... 0
Area LSA Count........................................... 1
IP Address.............................................. 2.2.2.2
OSPF Interface Events.................................... 1
Virtual Events........................................... 0
Neighbor Events.......................................... 0
External LSA Count...................................... 0
```

**show ip ospf lsa-group**

Use this command to display the number of self-originated LSAs within each LSA group.
Syntax

show ip ospf lsa-group [vrf vrf-name]

- vrf-name—The name of the VRF instance from which to display the self-originated LSA groups.

Default Configuration

There are no self-originated LSA groups by default.

Command Mode

Privileged Exec mode, Global Configuration mode, and all sub-modes

User Guidelines

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total self-originated LSAs</td>
<td>The number of LSAs the router is currently originating.</td>
</tr>
<tr>
<td>Average LSAs per group</td>
<td>The number of self-originated LSAs divided by the number of LSA groups. The</td>
</tr>
<tr>
<td></td>
<td>number of LSA groups is the refresh interval (1800 seconds) divided by the</td>
</tr>
<tr>
<td></td>
<td>pacing interval (configured with timers pacing lsa-group) plus two.</td>
</tr>
<tr>
<td>Pacing group limit</td>
<td>The maximum number of self-originated LSAs in one LSA group. If the number</td>
</tr>
<tr>
<td></td>
<td>of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout</td>
</tr>
<tr>
<td></td>
<td>the refresh interval to achieve better balance.</td>
</tr>
<tr>
<td>Groups</td>
<td>For each LSA pacing group, the output shows the range of LSA ages in the</td>
</tr>
<tr>
<td></td>
<td>group and the number of LSAs in the group.</td>
</tr>
</tbody>
</table>

Command History

Introduced in version 6.2.0.1 firmware.

Example

```
console#show ip ospf lsa-group

Total self-originated LSAs:  3019
Average LSAs per group:  100
```
Layer 3 Routing Commands

Pacing group limit: 400
Number of self-originated LSAs within each LSA group...

<table>
<thead>
<tr>
<th>Group Start Age</th>
<th>Group End Age</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>59</td>
<td>96</td>
</tr>
<tr>
<td>60</td>
<td>119</td>
<td>88</td>
</tr>
<tr>
<td>120</td>
<td>179</td>
<td>102</td>
</tr>
<tr>
<td>180</td>
<td>239</td>
<td>95</td>
</tr>
<tr>
<td>240</td>
<td>299</td>
<td>95</td>
</tr>
<tr>
<td>300</td>
<td>359</td>
<td>92</td>
</tr>
<tr>
<td>360</td>
<td>419</td>
<td>48</td>
</tr>
<tr>
<td>420</td>
<td>479</td>
<td>58</td>
</tr>
<tr>
<td>480</td>
<td>539</td>
<td>103</td>
</tr>
<tr>
<td>540</td>
<td>599</td>
<td>99</td>
</tr>
<tr>
<td>600</td>
<td>659</td>
<td>119</td>
</tr>
<tr>
<td>660</td>
<td>719</td>
<td>110</td>
</tr>
<tr>
<td>720</td>
<td>779</td>
<td>106</td>
</tr>
<tr>
<td>780</td>
<td>839</td>
<td>122</td>
</tr>
<tr>
<td>840</td>
<td>899</td>
<td>110</td>
</tr>
<tr>
<td>900</td>
<td>959</td>
<td>99</td>
</tr>
<tr>
<td>960</td>
<td>1019</td>
<td>135</td>
</tr>
<tr>
<td>1020</td>
<td>1079</td>
<td>101</td>
</tr>
<tr>
<td>1080</td>
<td>1139</td>
<td>94</td>
</tr>
<tr>
<td>1140</td>
<td>1199</td>
<td>115</td>
</tr>
<tr>
<td>1200</td>
<td>1259</td>
<td>110</td>
</tr>
<tr>
<td>1260</td>
<td>1319</td>
<td>111</td>
</tr>
</tbody>
</table>

**show ip ospf neighbor**

Use the **show ip ospf neighbor** command to display locally derived information about OSPF neighbors. The information below only displays if OSPF is enabled and the interface has a neighbor.

**Syntax**

```
show ip ospf neighbor [vrf vrf-name] [interface-type interface-number] [neighbor-id]
```

- **vrf-name** — The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- **interface-type** — Interface type – only supported type is vlan.
- **interface-number** — A valid interface number.
- **neighbor-id** — Valid IP address of the neighbor.
**Default Configuration**
This command has no default configuration.

**Command Mode**
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**
The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The following information is output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the interface on which the adjacency is formed.</td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td>The IPv4 address on the neighbor's interface used to form the adjacency.</td>
</tr>
<tr>
<td>Interface Index</td>
<td>The SNMP interface index.</td>
</tr>
<tr>
<td>Area Id</td>
<td>The OSPF area in which the adjacency is formed.</td>
</tr>
<tr>
<td>Options</td>
<td>The options advertised by the neighbor.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>The router priority advertised by the neighbor.</td>
</tr>
<tr>
<td>Dead timer</td>
<td>The number of seconds until the dead timer expires.</td>
</tr>
<tr>
<td>Up Time</td>
<td>How long this adjacency has been in FULL state.</td>
</tr>
<tr>
<td>State</td>
<td>The local state of the adjacency. The neighbor state is not tracked locally.</td>
</tr>
<tr>
<td>Events</td>
<td>Incremented for the following events:</td>
</tr>
<tr>
<td></td>
<td>• A DD is received from the neighbor with an MTU mismatch.</td>
</tr>
<tr>
<td></td>
<td>• The neighbor sent an ACK for an LSA not on the neighbor's retransmit list.</td>
</tr>
<tr>
<td></td>
<td>• The state of the adjacency changed.</td>
</tr>
<tr>
<td>Retransmitted LSAs</td>
<td>The number of LSAs retransmitted to a given neighbor.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retransmission Queue Length</td>
<td>The number of LSAs sent to the neighbor's retransmit queue waiting for the neighbor to acknowledge.</td>
</tr>
<tr>
<td>Restart Helper Status</td>
<td>One of two values:</td>
</tr>
<tr>
<td></td>
<td>• Helping — This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router's forwarding table is maintained during the restart.</td>
</tr>
<tr>
<td></td>
<td>• Not Helping — This router is not a helpful neighbor at this time.</td>
</tr>
</tbody>
</table>
Example

The following example displays locally derived information about OSPF neighbors on the specified Ethernet and IP interfaces.
show ip ospf range

Use the show ip ospf range command to display information about the area ranges for the specified area-id.

Syntax

show ip ospf range [vrf vrf-name] area-id

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- area-id —Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.
The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The following information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>The summary prefix.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnetwork mask of the summary prefix.</td>
</tr>
<tr>
<td>Type</td>
<td>S (Summary Link) or E (External Link)</td>
</tr>
<tr>
<td>Action</td>
<td>Advertise or Suppress</td>
</tr>
<tr>
<td>Cost</td>
<td>Metric to be advertised when the range is active. If a static cost is not configured, the field displays Auto. If the action is Suppress, the field displays N/A.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the range is currently active (Y) or not (N).</td>
</tr>
</tbody>
</table>

**Example**

The following example displays information about the area ranges configured for the specified area-id.

```
console#show ip ospf range 0
Prefix      Subnet Mask   Type     Action       Cost   Active
10.1.0.0      255.255.0.0      S  Advertise       Auto        N
172.20.0.0      255.255.0.0      S  Advertise        500        Y
```

**show ip ospf statistics**

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

**Syntax**

```
show ip ospf statistics [vrf vrf-name]
```

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

This command outputs the following.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>The time since the routing table was computed, in hours, minutes, and seconds (hh:mm:ss).</td>
</tr>
<tr>
<td>Intra</td>
<td>The time taken to compute intra-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Summ</td>
<td>The time taken to compute inter-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Ext</td>
<td>The time taken to compute external routes, in milliseconds.</td>
</tr>
<tr>
<td>SPF Total</td>
<td>The total time to compute routes, in milliseconds. The total may exceed the sum of the Intra, Summ, and Ext times.</td>
</tr>
<tr>
<td>RIB Update</td>
<td>The time from the completion of the routing table calculation until all changes have been made in the common routing table (the Routing Information Base, or RIB), in milliseconds.</td>
</tr>
<tr>
<td>Reason</td>
<td>The event or events that triggered the SPF. Reasons may include the following:</td>
</tr>
</tbody>
</table>

- R – New router LSA
- N – New network LSA
- SN – New network summary LSA
- SA – New ASBR summary LSA
- X – New external LSA
Example

console# show ip ospf statistics

Area 0.0.0.0: SPF algorithm executed 15 times

<table>
<thead>
<tr>
<th>Delta T</th>
<th>Intra</th>
<th>Summ</th>
<th>Ext</th>
<th>SPF Total</th>
<th>RIB Update</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:05:33</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:05:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:05:19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N, SN</td>
</tr>
<tr>
<td>00:05:15</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>R, N, SN</td>
</tr>
<tr>
<td>00:05:11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:04:50</td>
<td>0</td>
<td>60</td>
<td>0</td>
<td>60</td>
<td>460</td>
<td>R, N</td>
</tr>
<tr>
<td>00:04:46</td>
<td>0</td>
<td>90</td>
<td>0</td>
<td>100</td>
<td>60</td>
<td>R, N</td>
</tr>
<tr>
<td>00:03:42</td>
<td>0</td>
<td>70</td>
<td>10</td>
<td>90</td>
<td>160</td>
<td>R</td>
</tr>
<tr>
<td>00:03:39</td>
<td>0</td>
<td>70</td>
<td>40</td>
<td>120</td>
<td>240</td>
<td>X</td>
</tr>
<tr>
<td>00:03:36</td>
<td>0</td>
<td>60</td>
<td>60</td>
<td>130</td>
<td>160</td>
<td>X</td>
</tr>
<tr>
<td>00:01:28</td>
<td>0</td>
<td>60</td>
<td>50</td>
<td>130</td>
<td>240</td>
<td>X</td>
</tr>
<tr>
<td>00:01:25</td>
<td>0</td>
<td>30</td>
<td>50</td>
<td>110</td>
<td>310</td>
<td>SN</td>
</tr>
<tr>
<td>00:01:22</td>
<td>0</td>
<td>0</td>
<td>40</td>
<td>50</td>
<td>260</td>
<td>SN</td>
</tr>
<tr>
<td>00:01:19</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>20</td>
<td>190</td>
<td>X</td>
</tr>
<tr>
<td>00:01:16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>110</td>
<td>R, X</td>
</tr>
</tbody>
</table>

**show ip ospf stub table**

Use the `show ip ospf stub table` command to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

**Syntax**

`show ip ospf stub table [vrf vrf-name]`

- **vrf-name**—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

**Example**

The following example displays the OSPF stub table.

```console
console(config)#show ip ospf stub table
AreaId      TypeofService Metric Val Import SummaryLSA
------------- ------------- ---------- -----------------
0.0.0.1       Normal         1          Enable
```

**show ip ospf traffic**

Use the `show ip ospf traffic` command to display OSPFv2 packet and LSA statistics and OSPFv2 message queue statistics. Packet statistics count packets and LSAs since OSPFv2 counters were last cleared (using the `clear ip ospf counters` command.)

⚠️ **NOTE:** Note that the `clear ip ospf counters` command does not clear the message queue high water marks.

**Syntax**

`show ip ospf traffic [vrf vrf-name]`

- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches.

The `clear ip ospf counters` command does not clear the message queue high water marks.

The following is output.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv2 Packet Statistics</td>
<td>The number of packets of each type sent and received since OSPF counters were last cleared.</td>
</tr>
<tr>
<td>LSAs Retransmitted</td>
<td>The number of LSAs retransmitted by this router since OSPF counters were last cleared.</td>
</tr>
<tr>
<td>LS Update Max Receive Rate</td>
<td>The maximum rate of LS Update packets received during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.</td>
</tr>
<tr>
<td>LS Update Max Send Rate</td>
<td>The maximum rate of LS Update packets transmitted during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.</td>
</tr>
<tr>
<td>Number of LSAs Received</td>
<td>The number of LSAs of each type received since OSPF counters were last cleared.</td>
</tr>
<tr>
<td>OSPFv2 Queue Statistics</td>
<td>For each OSPFv2 message queue, the current count, the high water mark, the number of packets that failed to be enqueued, and the queue limit. The high water marks are not cleared when OSPF counters are cleared.</td>
</tr>
</tbody>
</table>

**Example**

```
console# show ip ospf traffic

Time Since Counters Cleared: 4000 seconds

OSPFv2 Packet Statistics

<table>
<thead>
<tr>
<th></th>
<th>Hello</th>
<th>Database</th>
<th>Desc</th>
<th>LS Request</th>
<th>LS Update</th>
<th>LS ACK</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recd:</td>
<td>500</td>
<td>10</td>
<td>20</td>
<td>50</td>
<td>20</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>Sent:</td>
<td>400</td>
<td>8</td>
<td>16</td>
<td>40</td>
<td>16</td>
<td>480</td>
<td></td>
</tr>
</tbody>
</table>
```
LSAs Retransmitted.................0
LS Update Max Receive Rate.........20 pps
LS Update Max Send Rate.............10 pps

Number of LSAs Received

T1 (Router).........................10
T2 (Network)........................0
T3 (Net Summary).....................300
T4 (ASBR Summary)...................15
T5 (External).........................20
T7 (NSSA External)...................0
T9 (Link Opaque)......................0
T10 (Area Opaque).....................0
T11 (AS Opaque)......................0
Total.................................345

OSPFv2 Queue Statistics

<table>
<thead>
<tr>
<th>Type</th>
<th>Current</th>
<th>Max</th>
<th>Drops</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>ACK</td>
<td>2</td>
<td>12</td>
<td>0</td>
<td>1680</td>
</tr>
<tr>
<td>Data</td>
<td>24</td>
<td>47</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>Event</td>
<td>1</td>
<td>8</td>
<td>0</td>
<td>1000</td>
</tr>
</tbody>
</table>

**show ip ospf virtual-links**

Use the `show ip ospf virtual-links` command to display the OSPF Virtual Interface information for a specific area and neighbor or for all neighbors.

**Syntax**

```
show ip ospf virtual-links [vrf vrf-name] [area-id neighbor-id]
```

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- area-id — Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0–4294967295)
- neighbor-id — Identifies the neighbor’s router ID. (Range: Valid IP address)

**Default Configuration**

Show information for all OSPF Virtual Interfaces.
**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100/N4000 series switches. OSPF must be enabled for this command to display the virtual interfaces.

**Example**

The following example displays the OSPF Virtual Interface information for area 10 and its neighbor.

```plaintext
console#show ip ospf virtual-links 10 192.168.2.2
Area ID.............................. 10
Neighbor Router ID.................. 192.168.2.2
Hello Interval....................... 10
Dead Interval........................ 655555
Iftransit Delay Interval............ 1
Retransmit Interval................ 5
State................................... down
Metric.................................. 0
Neighbor State....................... down
Authentication Type.................. MD5
Authentication Key.................... "test123"
Authentication Key ID............... 100
```

**show ip ospf virtual-links brief**

Use the `show ip ospf virtual-link brief` command to display the OSPF Virtual Interface information for all areas in the system in table format.

**Syntax**

`show ip ospf virtual-links brief`

**Default Configuration**

This command has no default configuration.
**Command Mode**
User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
OSPF must be enabled for this command to display the virtual interface information.

**Example**
The following example displays the OSPF Virtual Interface information in the system.

```
console#show ipv6 ospf virtual-link brief
```

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Neighbor</th>
<th>Hello Interval</th>
<th>Dead Interval</th>
<th>Retransmit Interval</th>
<th>Transit Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.2</td>
<td>5.5.5.5</td>
<td>10</td>
<td>40</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

timers pacing flood

Use the timers pacing flood command to adjust the rate at which OSPFv2 sends LS Update packets.
Use the no form of the command to return the timer pacing to the default value.

**Syntax**
timers pacing flood milliseconds
no timers pacing flood

- milliseconds—The average time between transmission of LS Update packets. The range is from 5 ms to 100 ms. The default is 33 ms.

**Default Configuration**
The default pacing between LS Update packets is 33 ms.

**Command Mode**
OSPFv2 Global Configuration mode
User Guidelines

OSPF distributes routing information in Link State Advertisements (LSAs), which are bundled into Link State Update (LS Update) packets. To reduce the likelihood of sending a neighbor more packets than it can buffer, OSPF rate limits the transmission of LS Update packets. By default, OSPF sends up to 30 updates per second on each interface (1/the pacing interval). Use this command to adjust the LS Update transmission rate.

**timers pacing lsa-group**

Use the `timers pacing lsa-group` command to tune how OSPF groups LSAs for periodic refresh.

**Syntax**

```plaintext
timers pacing lsa-group seconds
no timers pacing lsa-group
```

- `seconds`—Width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.

**Default Configuration**

The default timer pacing is 60 seconds.

**Command Mode**

OSPFv2 Global Configuration mode, OSPFv3 Global Configuration mode

**User Guidelines**

OSPF refreshes self-originated LSAs approximately once every 30 minutes. When OSPF refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPF to combine refreshed LSAs into a minimal number of Link-State packets. Minimizing the number of Link-State packets makes LSA distribution more efficient.

When OSPF originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPF refreshes the LSA. By selecting a random refresh delay, OSPF avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.
**Command History**

Command introduced in version 6.5 firmware.

**Example**

```
console(config-router6)#timers pacing lsa-group 90
```

**timers spf**

Use the `timers spf` command to configure the SPF delay and hold time. Use the no form of the command to reset the numbers to the default value.

**Syntax**

```
timers spf delay-time hold-time
no timers spf
```

- delay-time — SPF delay time. (Range: 0–65535 seconds)
- hold-time — SPF hold time. (Range: 0–65535 seconds)

**Default Configuration**

The default value for delay-time is 5. The default value for hold-time is 10.

**Command Mode**

Router OSPF Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures the SPF delay and hold time.

```
console(config-router)#timers spf 20 30
```
## OSPFv3 Commands

*Dell EMC Networking N3000/N3100/N4000 Series Switches*

Examples:

- **area default-cost**
- **area virtual-link transmit-delay**
- **ipv6 ospf priority**
- **show ipv6 ospf area**

- **area nssa (Router OSPFv3)**
- **default-information originate (Router OSPFv3 Configuration)**
- **ipv6 ospf retransmit-interval**
- **show ipv6 ospf asbr**

- **area nssa default-info-originate (Router OSPFv3 Config)**
- **default-metric**
- **ipv6 ospf transmit-delay**
- **show ipv6 ospf border-routers**

- **area nssa no-redistribute**
- **distance ospf**
- **ipv6 router ospf**
- **show ipv6 ospf database**

- **area nssa nosummary**
- **enable**
- **maximum-paths**
- **show ipv6 ospf database database-summary**

- **area nssa translator-role**
- **exit-overflow-interval**
- **nsf**
- **show ipv6 ospf interface**

- **area nssa translator-stab-intv**
- **external-lsdb-limit**
- **nsf helper**
- **show ipv6 ospf interface brief**

- **area range (Router OSPFv3)**
- **arp**
- **nsf helper strict-lsa-checking**
- **show ipv6 ospf interface stats**

- **area stub**
- **ipv6 ospf area**
- **nsf restart-interval**
- **show ipv6 ospf interface vlan**

- **area stub no-summary**
- **ipv6 ospf cost**
- **passive-interface**
- **show ipv6 ospf neighbor**

- **area virtual-link**
- **ipv6 ospf dead-interval**
- **passive-interface default**
- **show ipv6 ospf range**

---

*The Dell Network N1500/N2000/N2100-ON series support limited routing and multicast capabilities. See the Users Configuration Guide section “Feature Limitations and Platform Constants” for supported capabilities.*

This section explains the following commands:
area default-cost (Router OSPFv3)

Use the area default-cost command in Router OSPFv3 Configuration mode to configure the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215. Use the no form of the command to return the cost to the default value. If the area has not been previously created, this command creates the area and then applies the default-cost.

**Syntax**

```
area area-id default-cost cost
no area area-id default-cost
```

- **areaid** — Valid area identifier.
- **cost** — Default cost. (Range: 1-16777215)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Router OSPFv3 Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example configures the monetary default cost at 100 for stub area 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 default-cost 100
```

area nssa (Router OSPFv3)
Use the `area nssa` command in Router OSPF Configuration mode to configure the specified area ID to function as an NSSA. If the area has not been previously created, this command creates the area and then applies the NSSA distinction. If the area already exists, the NSSA distinction is added or modified. Use the `no` form of the command to remove the NSSA distinction from the area.

Syntax
```
area area-id nssa [no-redistribution] [default-information originate [metric metric-value] [metric-type metric-type-value]] [no-summary] [translator-role role] [translator-stab-intv interval]
```
```
no area area-id nssa [no-redistribution] [default-information originate] [no-summary] [translator-role] [translator-stab-intv]
```

- `area-id`—Identifies the OSPFv3 stub area to configure. (Range: IP address or decimal from 0–4294967295)
- `metric-value`—Specifies the metric of the default route advertised to the NSSA. (Range: 1–16777214)
- `metric-type-value`—The metric type can be one of the following:
  - A metric type of nssa-external 1 (comparable)
  - A metric type of nssa-external 2 (non-comparable)
- `role`—The translator role where role is one of the following:
  - `always` - The router assumes the role of the translator when it becomes a border router.
  - `candidate` - The router to participate in the translator election process when it attains border router status.
• interval—The period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. (Range: 0–3600)

**Default Configuration**

If no metric is defined, 10 is the default configuration.

The default role is candidate.

**Command Mode**

Router OSPFv3 Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures not-so-stubby-area 10 as an NSSA.

```
console(config)#ipv6 router ospf
console(config-router)#area 10 nssa
```

The following example configures the metric value and type for the default route advertised into the NSSA and configures the NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config-router)#area 20 nssa default-info-originate metric 250
metric-type 2 no-summary
```

**area nssa default-info-originate (Router OSPFv3 Config)**

Use the `area nssa default-info-originate` command in Router OSPFv3 Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route. The metric type can be comparable (`nssa-external 1`) or noncomparable (`nssa-external 2`). Use the `no` form of the command to return the metric value and type to the default value.
Syntax
area areaid nssa default-info-originate [metric [comparable | non-comparable]]
no area areaid nssa default-info-originate
• areaid — Valid OSPFv3 area identifier.
• metric — Metric value for default route. (Range: 1-16777214)
• comparable — Metric Type (nssa-external 1).
• non-comparable — Metric Type (nssa-external 2).

Default Configuration
If no metric is defined, 10 is the default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example configures the default metric value for the default route advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa default-info-originate
```

area nssa no-redistribute
Use the area nssa no-redistribute command in Router OSPFv3 Configuration mode to configure the NSSA ABR so that learned external routes will not be redistributed to the NSSA. Use the no form of the command to remove the configuration.

Syntax
area areaid nssa no-redistribute
no area areaid nssa no-redistribute
• areaid — Valid OSPF area identifier.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Router OSPFv3 Configuration mode.

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures the area 1 NSSA ABR so that learned external routes will not be redistributed to the NSSA.

```console
console(config)#ipv6 router ospf
crsole(config-rtr)#area 1 nssa no-redistribute
```

**area nssa no-summary**
Use the `area nssa no-summary` command in Router OSPFv3 Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA. Use the no form of the command to remove the configuration.

**Syntax**
```
area areaid nssa no-summary
no area area-id nssa no-summary
```
• areaid — Valid OSPF area identifier.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Router OSPFv3 Configuration mode.
User Guidelines
This command has no user guidelines.

Example
The following example configures the area 1 NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa no-summary
```

area nssa translator-role
Use the area nssa translator-role command in Router OSPFv3 Configuration mode to configure the translator role of the NSSA. Use the no form of the command to remove the configuration.

Syntax
```
area areaid nssa translator-role {always | candidate}
```
```
no area areaid nssa translator-role
```
- **areaid** — Valid OSPF area identifier.
- **always** — Causes the router to assume the role of the translator the instant it becomes a border router.
- **candidate** — Causes the router to participate in the translator election process when it attains border router status.

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.
Example
The following example configures the always translator role of the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa translator-role always
```

area nssa translator-stab-intv

Use the `area nssa translator-stab-intv` command in Router OSPFv3 Configuration mode to configure the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Syntax
```
area areaid nssa translator-stab-intv seconds
no area areaid nssa translator-stab-intv
```

- `areaid` — Valid OSPF area identifier.
- `seconds` — Translator stability interval of the NSSA. (Range: 0-3600 seconds)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example configures a translator stability interval of 100 seconds for the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa translator-stab-intv 100
```
area range (Router OSPFv3)

Use the area range command in Router OSPF Configuration mode to configure a summary prefix for routes learned in a given area. If the area has not been previously created, this command creates the area and then applies the range parameters. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA. Use the no form of the command to remove the summary prefix configuration for routes learned in the specified area.

**Syntax**

area area-id range ipv6-prefix/prefix-length {summarylink | nssaexternallink} [advertise | not-advertise]

no area area-id range ipv6-prefix/prefix-length {summarylink | nssaexternallink}

- areaid—Valid OSPFv3 area identifier.
- ipv6-prefix/prefix-length—Valid route prefix.
- summarylink—LSDB type
- nssaexternallink—LSDB type.
- advertise—Allows area range to be advertised.
- not-advertise—Suppresses area range from being advertised.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Router OSPFv3 Configuration mode.

**User Guidelines**

The LSDB type must be specified by either summarylink or nssaexternallink, and the advertising of the area range can be allowed or suppressed.
Example
The following example creates an area range for the area 1 NSSA.

```console
console(config)#ipv6 router ospf
console(config-rtr)#area 1 range 2020::1::1/64 summarylink
```

**area stub**

Use the `area stub` command in Router OSPFv3 Configuration mode to create a stub area for the specified area ID. If the area has not been previously created, this command creates the area and then applies the stub distinction. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the size of the link state database of routers within the stub area.

**Syntax**

```
area area-id stub [no summary]
```

```
no area area-id stub [no summary]
```

- `area-id` — Valid OSPFv3 area identifier.
- `no-summary`—Disable the import of Summary LSAs for the stub area identified by area-id.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Router OSPFv3 Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example creates a stub area for area 1.

```console
console(config)#ipv6 router ospf
console(config-rtr)#area 1 stub
```
area stub no-summary

Use the area stub no-summary command in Router OSPFv3 Configuration mode disable the import of Summary LSAs for the stub area identified by area-id.

Syntax
area area-id stub no-summary
no area area-id stub no-summary

- area-id — Valid OSPFv3 area identifier.
- so-summary — Disable the import of Summary LSAs for the stub area identified by area-id.

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example prevents Summary LSAs from being advertised into the area 1 NSSA.

console(config)#ipv6 router ospf
console(config-rtr)#area 1 stub no-summary

area virtual-link

Use the area virtual-link command in Router OSPFv3 Configuration mode to create the OSPF virtual interface for the specified area-id and neighbor router. If the area has not been previously created, this command creates the area and then applies the virtual-link parameters. To remove the link, use the no form of the command. Use the optional parameters to configure dead-interval, hello-interval, retransmit-interval and transmit-delay.
**Syntax**

```
area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds]
no area area-id virtual-link router-id id [hello-interval] [retransmit-interval] [transmit-delay] [dead-interval]
```

- **area-id**—Valid OSPFv3 area identifier (or decimal value in the range of 0-4294967295).
- **router-id**—Identifies the Router ID or valid IP address of the neighbor.
- **hello-interval** seconds—Number of seconds to wait before sending hello packets to the OSPF virtual interface. (Range: 1–65535)
- **dead-interval** seconds—Number of seconds to wait before the OSPF virtual interface on the virtual interface is assumed to be dead. (Range: 1–65535)
- **retransmit-interval** seconds—The number of seconds to wait between retransmitting LSAs if no acknowledgment is received. (Range: 0–3600)
- **transmit-delay** seconds—Number of seconds to increment the age of the LSA before sending, based on the estimated time it takes to transmit from the interface. (Range: 0–3600)

**Default Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>No area ID is predefined.</td>
</tr>
<tr>
<td>router-id</td>
<td>No router ID is predefined.</td>
</tr>
<tr>
<td>hello-interval seconds</td>
<td>10 seconds</td>
</tr>
<tr>
<td>retransmit-interval seconds</td>
<td>5 seconds</td>
</tr>
<tr>
<td>transmit-delay seconds</td>
<td>1 second</td>
</tr>
<tr>
<td>dead-interval seconds</td>
<td>40 seconds</td>
</tr>
</tbody>
</table>
**Command Mode**
Router OSPFv3 Configuration mode.

**User Guidelines**
This command has no user guidelines.

**Example**
The following example creates the OSPF virtual interface for area 1 and its neighbor router.

```
consule(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2
```

The following example configures a 20-second dead interval, a hello interval of 20 seconds, a retransmit interval of 20 seconds, and a 20-second transmit delay for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
consule(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 dead-interval 20 hello-interval 20 retransmit-interval 20 transmit-delay 20
```

**area virtual-link dead-interval**
Use the `area virtual-link dead-interval` command in Router OSPFv3 Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.

**Syntax**
```plaintext
area areaid virtual-link neighbor dead-interval seconds
no area areaid virtual-link neighbor dead-interval
```

- **areaid** — Valid OSPFv3 area identifier.
- **neighbor** — Router ID of neighbor.
- **seconds** — Dead interval. (Range: 1-65535)

**Default Configuration**
40 is the default value for seconds.
Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example configures a 20-second dead interval for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
crshell(config)#ipv6 router ospf
crshell(config-rtr)#area 1 virtual-link 2 dead-interval 20
```

`area virtual-link hello-interval`

Use the `area virtual-link hello-interval` command in Router OSPFv3 Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.

Syntax
```
area areaid virtual-link neighbor hello-interval seconds
no area areaid virtual-link neighbor hello-interval
```

- areaid — Valid OSPFv3 area identifier.
- neighbor — Router ID of neighbor.
- seconds — Hello interval. (Range: 1-65535)

Default Configuration
10 is the default value for seconds.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.
Example
The following example configures a hello interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 hello-interval 20
```

**area virtual-link retransmit-interval**

Use the `area virtual-link retransmit-interval` command in Router OSPFv3 Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.

**Syntax**

```
area areaid virtual-link neighbor retransmit-interval seconds
```

```
no area areaid virtual-link neighbor retransmit-interval
```

- areaid — Valid OSPFv3 area identifier.
- neighbor — Router ID of neighbor.
- seconds — Retransmit interval. (Range: 0-3600)

**Default Configuration**

5 is the default value for seconds.

**Command Mode**

Router OSPFv3 Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures the retransmit interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
(config)#ipv6 router ospf
(config-rtr)#area 1 virtual-link 2 retransmit-interval 20
```
area virtual-link transmit-delay

Use the area virtual-link transmit-delay command in Router OSPFv3 Configuration mode to configure the transmit delay for the OSPF virtual interface on the virtual interface identified by areaid and neighbor.

Syntax

area areaid virtual-link neighbor transmit-delay seconds
no area areaid virtual-link neighbor transmit-delay

• areaid — Valid OSPFv3 area identifier.
• neighbor — Router ID of neighbor.
• seconds — Transmit delay interval. (Range: 0-3600)

Default Configuration

1 is the default value for seconds.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 20-second transmit delay for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 transmit-delay 20

default-information originate (Router OSPFv3 Configuration)

Use the default-information originate command in Router OSPFv3 Configuration mode to control the advertisement of default routes. Use the no form of the command to return the default route advertisement settings to the default value.
Syntax

default-information originate [always] [metric metric-value] [metric-type type-value]

no default-information originate [metric] [metric-type]

- always—Always advertise default routes.
- metric-value—
- type-value—The metric (or preference) value of the default route. (Range: 1–16777214)

- One of the following:
  1 External type-1 route.
  2 External type-2 route.

Default Configuration

The default metric is none and the default type is 2.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example controls the advertisement of default routes by defining a metric value of 100 and metric type 2.

```
console(config)#ipv6 router ospf
cnsole(config-rtr)#default-information originate metric 100 metric-type 2
```

default-metric

Use the default-metric command in Router OSPFv3 Configuration mode to set a default for the metric of distributed routes. Use the no form of the command to remove the metric from the distributed routes.
Syntax
default-metric metric-value
no default-metric

• metric-value — The metric (or preference) value of the default route.
  (Range: 1–16777214)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets a default of 100 for the metric of distributed routes.

```
console(config)#ipv6 router ospf
console(config-rtr)#default-metric 100
```

**distance ospf**

The `distance ospf` command sets the preference values of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, external. All the external type routes are given the same preference value. Use the “no” form of this command to reset the preference values to the default.

Syntax

distance ospf {external | inter-area | intra-area} distance

no distance ospf {external | inter-area | intra-area} distance

• distance—Used to select the best path when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).
**Default Configuration**
The default preference value is 110.

**Command Mode**
Router OSPF Configuration mode.
Router OSPFv3 Configuration mode.

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example sets a route preference value of 100 for intra OSPF in the router.

```
console(config)#ipv6 router ospf
console(config-rtr)#distance ospf intra 100
```

**enable**
Use the `enable` command in Router OSPFv3 Configuration mode to enable administrative mode of OSPF in the router (active).

**Syntax**
```
enable
no enable
```

**Default Configuration**
Enabled is the default state.

**Command Mode**
Router OSPFv3 Configuration mode.

**User Guidelines**
This command has no user guidelines.
**Example**
The following example enables administrative mode of OSPF in the router (active).
```
console(config)#ipv6 router ospf
console(config-rtr)#enable
```

**exit-overflow-interval**
Use the `exit-overflow-interval` command in Router OSPFv3 Configuration mode to configure the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to originate non-default AS-external-LSAs again. When set to 0, the router will not leave Overflow State until restarted.

**Syntax**
```
exit-overflow-interval seconds
no exit-overflow-interval
```
- `seconds` — Exit overflow interval for OSPF (Range: 0-2147483647)

**Default Configuration**
0 is the default value for seconds.

**Command Mode**
Router OSPFv3 Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures the exit overflow interval for OSPF at 100 seconds.
```
console(config)#ipv6 router ospf
console(config-rtr)#exit-overflow-interval 100
```
**external-lsdb-limit**

Use the `external-lsdb-limit` command in Router OSPFv3 Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in its database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

**Syntax**

`external-lsdb-limit` limit  
`no external-lsdb-limit`  
- limit — External LSDB limit for OSPF (Range: -1-2147483647)

**Default Configuration**

-1 is the default value for limit.

**Command Mode**

Router OSPFv3 Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the external LSDB limit at 100 for OSPF.

```plaintext
console(config)#ipv6 router ospf
console(config-rtr)#external-lsdb-limit 100
```

**ipv6 ospf**

Use the `ipv6 ospf` command in Interface Configuration mode to enable OSPF on a router interface or loopback interface.
**Syntax**

ipv6 ospf
no ipv6 ospf

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example enables OSPF on VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf
```

**ipv6 ospf area**

Use the `ipv6 ospf area areaid` command in Interface Configuration mode to set the OSPF area to which the specified router interface belongs.

**Syntax**

ipv6 ospf area areaid
no ipv6 ospf area areaid

- areaid — Is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value. It uniquely identifies the area to which the interface connects. Assigning an area id which does not exist on an interface causes the area to be created with default values. (Range: 0-4294967295).

**Default Configuration**

This command has no default configuration.
**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example defines the OSPF area to which VLAN 15 belongs.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf area 100
```

**ipv6 ospf cost**

Use the `ipv6 ospf cost` command in Interface Configuration mode to configure the cost on an OSPF interface. Use the `no` form of the command to return the cost to the default value.

**Syntax**

```
ipv6 ospf cost interface-cost
no ipv6 ospf cost
```

- `interface-cost` — Specifies the cost (link-state metric) of the OSPF interface. (Range: 1–65535)

**Default Configuration**

10 is the default link-state metric configuration.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example configures a cost of 100.

```
console(config)#interface vlan 15
```
console(config-if-vlan15)#ipv6 ospf cost 100

**ipv6 ospf dead-interval**

Use the `ipv6 ospf dead-interval` command in Interface Configuration mode to set the OSPF dead interval for the specified interface.

**Syntax**

ipv6 ospf dead-interval seconds

no ipv6 ospf dead-interval

- seconds — A valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). (Range: 1-65535)

**Default Configuration**

40 seconds is the default value of seconds.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the OSPF dead interval at 100 seconds.

console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf dead-interval 100

**ipv6 ospf hello-interval**

Use the `ipv6 ospf hello-interval` command in Interface Configuration mode to set the OSPF hello interval for the specified interface.
**Syntax**

ipv6 ospf hello-interval seconds

no ipv6 ospf hello-interval

- seconds — A valid positive integer which represents the length of time of the OSPF hello interval. The value must be the same for all routers attached to a network. (Range: 1-65535 seconds)

**Default Configuration**

10 seconds is the default value of seconds.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the OSPF hello interval at 15 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf hello-interval 15
```

**ipv6 ospf mtu-ignore**

Use the `ipv6 ospf mtu-ignore` command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. Use the `no` form of the command to reset mismatch detection to the default value.

**Syntax**

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

**Default Configuration**

The default state is Disabled.
Command Mode
Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines
OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Example
The following example disables OSPF maximum transmission unit (MTU) mismatch detection.

console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf mtu-ignore

ipv6 ospf network
Use the ipv6 ospf network command in Interface Configuration mode to change the default OSPF network type for the interface. Use the no form of the command to return the network setting to the default value.

Syntax
ipv6 ospf network {broadcast | point-to-point}
no ipv6 ospf network
  •  broadcast — The network type is broadcast.
  •  point-to-point — The network type is point-to-point.

Default Configuration
The default state is point-to-point.

Command Mode
Interface Configuration (VLAN, Tunnel, Loopback) mode
**User Guidelines**

Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF-type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

**Example**

The following example changes the default OSPF network type to point-to-point.

```plaintext
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf network point-to-point
```

**ipv6 ospf priority**

Use the `ipv6 ospf priority` command in Interface Configuration mode to set the OSPF priority for the specified router interface. Use the `no` form of the command to return the priority to the default value.

**Syntax**

`ipv6 ospf priority number-value`

`no ipv6 ospf priority`

- number-value — Specifies the OSPF priority for the specified router interface. (Range: 0–255) A value of 0 indicates that the router is not eligible to become the designated router on this network.

**Default Configuration**

1, the highest router priority, is the default value.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.
**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the OSPF priority at 50 for VLAN 15.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf priority 50
```

**ipv6 ospf retransmit-interval**

Use the `ipv6 ospf retransmit-interval` command in Interface Configuration mode to set the OSPF retransmit interval for the specified interface.

**Syntax**

```plaintext
ipv6 ospf retransmit-interval 
no ipv6 ospf retransmit-interval 
```

- `seconds` — The number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0 to 3600 seconds)

**Default Configuration**

5 seconds is the default value.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the OSPF retransmit interval at 100 seconds.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf retransmit-interval 100
```
**ipv6 ospf transmit-delay**

Use the `ipv6 ospf transmit-delay` command in Interface Configuration mode to set the OSPF Transmit Delay for the specified interface.

**Syntax**

```plaintext
ipv6 ospf transmit-delay seconds
no ipv6 ospf transmit-delay
```

- `seconds` — OSPF transmit delay for the specified interface. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1 to 3600 seconds)

**Default Configuration**

No default value.

**Command Mode**

Interface Configuration (VLAN, Tunnel, Loopback) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets the OSPF Transmit Delay at 100 seconds for VLAN 15.

```plaintext
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf transmit-delay 100
```

**ipv6 router ospf**

Use the `ipv6 router ospf` command in Global Configuration mode to enable OSPFv3 and enter Router OSPFv3 Configuration mode. Use the `no` form of the command to disable OSPFv3 and remove the OSPFv3 interface and global configuration.

**Syntax**

```plaintext
ipv6 router ospf
```
no ipv6 router ospf

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode.

**User Guidelines**
This command has no user guidelines.

**Example**
Use the following command to enable OSPFv3.

```
console(config)#ipv6 router ospf
```

**maximum-paths**
Use the `maximum-paths` command in Router OSPFv3 Configuration mode to set the number of paths that OSPF can report for a given destination.

**Syntax**

```
maximum-paths maxpaths
no maximum-paths
```

- `maxpaths` — Number of paths that can be reported. (Range: 1-2)

**Default Configuration**
2 is the default value for maxpaths.

**Command Mode**
Router OSPFv3 Configuration mode.

**User Guidelines**
This command has no user guidelines.
Example
The following example sets the number of paths that OSPF can report for a
destination to 1.

console(config)#ipv6 router ospf
console(config-rtr)#maximum-paths 1

nsf
Use this command to enable OSPF graceful restart. Use the no form of this
command to disable graceful restart.

Syntax
nsf [ietf] [planned-only]
no nsf [ietf]

• ietf — This keyword is used to distinguish the IETF standard
  implementation of graceful restart from other implementations. Since the
  IETF implementation is the only one supported, this keyword is optional.

• planned-only — This keyword indicates that OSPF should only perform a
  graceful restart when the restart is planned (i.e., when the restart is a result
  of the initiate failover command).

Default Configuration
Graceful restart is disabled by default

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
Graceful restart works in concert with nonstop forwarding to enable the
hardware to continue forwarding IPv6 packets using OSPFv3 routes while a
backup unit takes over management unit responsibility. When OSPF
executes a graceful restart, it informs its neighbors that the OSPF control
plane is restarting, but that it will be back shortly. Helpful neighbors continue
to advertise to the rest of the network that they have full adjacencies with the
restarting router, avoiding announcement of a topology change and
everything that goes with that (i.e., flooding of LSAs, SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors. This implementation of graceful restart restarting router behavior is only useful with a router stack. Graceful restart does not work on a standalone, single-unit router.

**nsf helper**

Use the `nsf-helper` to allow OSPF to act as a helpful neighbor for a restarting router. Use the `no` form of this command to prevent OSPF from acting as a helpful neighbor.

**Syntax**

```
nsf helper[planned-only]
no nsf helper
```

- `planned-only` — This keyword indicates that OSPF should only help a restarting router performing a planned restart.

**Default Configuration**

OSPF may act as a helpful neighbor for both planned and unplanned restarts.

**Command Mode**

Router OSPFv3 Configuration mode

**User Guidelines**

The grace LSA announcing the graceful restart includes a restart reason. Reasons 1 (software restart) and 2 (software reload/upgrade) are considered planned restarts. Reasons 0 (unknown) and 3 (switch to redundant control processor) are considered unplanned restarts.

`nsf ietf helper disable` is functionally equivalent to `no nsf helper` and is supported solely for IS CLI compatibility.
**nsf helper strict-lsa-checking**

Use the `nsf-helper strict-lsa-checking` command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the “no” form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

**Syntax**

```
nsf [ietf] helper strict-lsa-checking
no nsf [ietf] helper strict-lsa-checking
```

- `ietf` — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

**Default Configuration**

A helpful neighbor exits helper mode when a topology change occurs.

**Command Mode**

Router OSPFv3 Configuration mode

**User Guidelines**

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router.

A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

**nsf restart-interval**

Use the `nsf restart-interval` command to configure the length of the grace period on the restarting router. Use the “no” form of this command to revert the grace period to its default.
**Syntax**

nsf [ietf] restart-interval seconds

no nsf [ietf] restart-interval

- ietf — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

- seconds — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1–1800 seconds).

**Default Configuration**

The default restart interval is 120 seconds.

**Command Mode**

Router OSPFv3 Configuration mode

**User Guidelines**

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

**passive-interface**

Use the passive-interface command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel. Use the “no” form of this command to set the interface or tunnel as non-passive.

**Syntax**

passive-interface {vlan vlan-id | tunnel tunnel-id}

no passive-interface {vlan vlan-id | tunnel tunnel-id}

- vlan-id — The VLAN number
- tunnel-id — Tunnel identifier. (Range: 0–7)
Default Configuration
Passive interface mode is disabled by default.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-router)#passive-interface vlan 1

passive-interface default
The passive-interface default command enables the global passive mode by default for all interfaces. It overrides any interface level passive mode. Use the “no” form of this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Syntax
passive-interface default
no passive-interface default

Default Configuration
Global passive mode is disabled by default.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
There are no user guidelines for this command.

Example
console(config-rtr)#passive-interface default
redistribute (OSPFv3)

Use the `redistribute` command in Router OSPFv3 Configuration mode to configure the OSPFv3 protocol to allow redistribution of routes from the specified sources.

**Syntax**

```
redistribute protocol [metric metric-value] [tag tag-value] [route-map route-tag]
```

```
no redistribute protocol
```

- **protocol** — One of the following:
  - `static` — Specifies that static routes are to be redistributed.
  - `connected` — Specifies that connected routes are to be redistributed.
  - `bgp` — Specifies BGP originated routes are to be redistributed.

- **metric-value** — Metric value used for default routes. (Range: 0-16777214)

- **tag-value** — Insert the specified tag value into redistributed routes.

- **route-tag** — Filter redistributed routes using the specified route map.

**Default Configuration**

The default tag value is 0.

There is no default metric or route map configured.

**Command Mode**

Router OSPFv3 Configuration mode

**User Guidelines**

When redistributing a route metric, the receiving protocol must understand the metric. The OSPF metric is a cost value equal to $10^8$/ link bandwidth in bits/sec. For example, the OSPF cost of GigabitEthernet is $1 = 10^8/10^8 = 1$.

The RIP metric is a hop count with a maximum value of 15. Redistribution of BGP-originated routes is only available on BGP-enabled routers.
Example
The following example configures the OSPFv3 protocol to allow redistribution of routes to connected devices.

console(config)#ipv6 router ospf
console(config-rtr)#redistribute connected

router-id
Use the router-id command in Router OSPFv3 Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.

Syntax
router-id router-id
  • router-id — Router OSPF identifier. (Range: 0-4294967295)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets a 4-digit dotted-decimal number identifying the Router OSPF ID as 2.3.4.5.

console(config)#ipv6 router ospf
console(config-rtr)#router-id 2.3.4.5

show ipv6 ospf
Use the show ipv6 ospf command to display information relevant to the OSPF router.
**Syntax**

```
show ipv6 ospf [area-id]
```

*area-id* — Identifier for the OSPF area being displayed.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Shows whether OSPF is administratively enabled or disabled.</td>
</tr>
<tr>
<td>External LSDB Limit</td>
<td>Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.</td>
</tr>
<tr>
<td>Exit Overflow Interval</td>
<td>Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.</td>
</tr>
<tr>
<td>AutoCost Ref BW</td>
<td>The configured autocost reference bandwidth. This value is used to determine the OSPF metric on its interfaces. The reference bandwidth is divided by the interface speed to compute the metric.</td>
</tr>
<tr>
<td>Default Passive Setting</td>
<td>When enabled, OSPF interfaces are passive by default.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>Shows the maximum number of paths that OSPF can report for a given destination.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>Default metric for redistributed routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>When enabled, OSPF originates a type 5 LSA advertising a default route.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Always</td>
<td>When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.</td>
</tr>
<tr>
<td>Metric</td>
<td>Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.</td>
</tr>
<tr>
<td>Number of Active Areas</td>
<td>The number of OSPF areas to which the router is attached on interfaces that are up.</td>
</tr>
<tr>
<td>ABR Status</td>
<td>Shows whether the router is an OSPF Area Border Router.</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Indicates whether the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from another protocol. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).</td>
</tr>
<tr>
<td>Stub Router</td>
<td>OSPF enters stub router mode, as described in RFC 3137, when it encounters a resource limitation that prevents it from computing a complete routing table. In this state, OSPF sets the link metrics of non-stub links in its own router LSAs to the largest possible value, discouraging other routers from computing paths through the stub router, but allowing other routers to compute routes to destinations attached to the stub router. To restore OSPF to normal operation, resolve the condition that caused the resource overload, then disable and reenable OSPF globally.</td>
</tr>
<tr>
<td>External LSDB Overflow</td>
<td>OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.</td>
</tr>
<tr>
<td>External LSA Count</td>
<td>Shows the number of external (LS type 5) link-state advertisements in the link-state database.</td>
</tr>
<tr>
<td>External LSA Checksum</td>
<td>Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.</td>
</tr>
<tr>
<td>New LSAs Originated</td>
<td>Shows the number of link-state advertisements that have been originated.</td>
</tr>
<tr>
<td><strong>LSAs Received</strong></td>
<td>Shows the number of link-state advertisements received determined to be new instantiations.</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>LSA Count</strong></td>
<td>The number of LSAs in the link state database.</td>
</tr>
<tr>
<td><strong>Maximum Number of LSAs</strong></td>
<td>The limit on the number of LSAs that the router can store in its link state database.</td>
</tr>
<tr>
<td><strong>LSA High Water Mark</strong></td>
<td>The maximum number of LSAs that have been in the link state database since OSPF began operation.</td>
</tr>
<tr>
<td><strong>Retransmit List Entries</strong></td>
<td>The current number of entries on all neighbors’ retransmit lists.</td>
</tr>
<tr>
<td><strong>Maximum Number of Retransmit Entries</strong></td>
<td>The maximum number of entries that can be on neighbors’ retransmit lists at any given time. This is the sum for all neighbors. When OSPF receives an LSA and cannot allocate a new retransmit list entry, the router does not acknowledge the LSA, expecting the sender to retransmit.</td>
</tr>
<tr>
<td><strong>Retransmit Entries High Water Mark</strong></td>
<td>The maximum number of retransmit list entries that have been on all neighbors’ retransmit lists at one time.</td>
</tr>
<tr>
<td><strong>NSF Support</strong></td>
<td>Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.</td>
</tr>
<tr>
<td><strong>NSF Restart Interval</strong></td>
<td>The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.</td>
</tr>
<tr>
<td><strong>NSF Restart Status</strong></td>
<td>Whether the router is currently performing a graceful restart.</td>
</tr>
<tr>
<td><strong>NSF Restart Age</strong></td>
<td>The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.</td>
</tr>
<tr>
<td><strong>NSF Restart Exit Reason</strong></td>
<td>The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.</td>
</tr>
<tr>
<td><strong>NSF Helper Support</strong></td>
<td>Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.</td>
</tr>
<tr>
<td><strong>NSF Helper Strict LSA Checking</strong></td>
<td>As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor’s graceful restart.</td>
</tr>
<tr>
<td><strong>Redistributing</strong></td>
<td>This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.</td>
</tr>
</tbody>
</table>
Layer 3 Routing Commands

Example

The following example enables OSPF traps.

```console
(console)# show ipv6 ospf
Router ID................................. 0.0.0.2
OSPF Admin Mode......................... Enable
ASBR Mode................................. Disable
ABR Status................................. Disable
Exit Overflow Interval.................... 0
External LSA Count........................ 0
External LSA Checksum..................... 0
New LSAs Originated....................... 0
LSAs Received............................. 0
External LSDB Limit....................... No Limit
Default Metric............................ Not Configured
Maximum Paths............................. 2
Default Route Advertise................... Disabled
Always..................................... FALSE
Metric......................................
Metric Type.................................. External Type 2
NSF Support................................. Disabled
NSF Restart Interval....................... 120 seconds
NSF Helper Support......................... Always
NSF Helper Strict LSA Checking............ Enabled
```

**show ipv6 ospf abr**

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

**Syntax**

```
show ipv6 ospf abr
```

**Default Configuration**

This command has no default configuration.
**Command Mode**
User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
```
cmdshow ipv6 ospf abr
Type Router Id Cost Area ID Next Hop Next Hop
----- -------- ---- -------- ---------------------- -------
INTRA 3.3.3.3 10 0.0.0.1 FE80::211:88FF:FE2A:3CB3 vlan11
INTRA 4.4.4.4 10 0.0.0.1 FE80::210:18FF:FE82:8E1 vlan12
```

**show ipv6 ospf area**
Use the **show ipv6 ospf area** command to display information about the area.

**Syntax**
```
show ipv6 ospf area areaid
```
- **areaid** — Identifier for the OSPF area being displayed.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays information about area 1.
```
cmdshow ipv6 ospf area 1
```
show ipv6 ospf asbr

The `show ipv6 ospf asbr` command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax

```
show ipv6 ospf asbr
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf asbr
    Type   Router Id   Cost  Area ID   Next Hop                Intf
    ------   ---------   ----  --------  -----------------------  ----
    INTRA   1.1.1.1     10     0.0.0.1  FE80::213:C4FF:FEDB:6C41  vlan10
    INTRA   4.4.4.4     10     0.0.0.1  FE80::210:18FF:FE82:8E1    vlan12
```

show ipv6 ospf border-routers

Use the `show ipv6 ospf` command to display internal OSPFv3 routes to reach Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR). This command takes no options.
Syntax

show ipv6 ospf border-routers

Default Configuration

This command has no default configuration.

Command Mode

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**show ipv6 ospf database**

Use the `show ipv6 ospf database` command to display information about the link state database when OSPFv3 is enabled.

Syntax

```
show ipv6 ospf [area-id] database [{external | inter-area {prefix | router} | link | network | nssaexternal | prefix | router | unknown [area | as | link]}] [link-state-id] [adv-router [router-id] | self-originate]
```

- area-id — Identifies a specific OSPF area for which link state database information will be displayed.
- external — Displays the external LSAs.
- inter-area — Displays the inter-area LSAs.
- link — Displays the link LSAs.
- network — Displays the network LSAs.
- nssa-external — Displays NSSA external LSAs.
- prefix — Displays intra-area Prefix LSA.
- router — Displays router LSAs.
- unknown — Displays unknown area, AS or link-scope LSAs.
- link-state-id — Specifies a valid link state identifier (LSID).
- adv-router — Shows the LSAs that are restricted by the advertising router.
- router-id — Specifies a valid router identifier.
- self-originate — Displays the LSAs in that are self originated.
**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

If no parameters are entered, the command displays the LSA headers. Optional parameters specify the type of link state advertisements to display. The information below is only displayed if OSPF is enabled.

**Example**

The following example displays information about the link state database when OSPFv3 is enabled.

```
console#show ipv6 ospf database

Router Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Adv Router</th>
<th>Link Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Csum</th>
<th>Options</th>
<th>Rtr</th>
<th>Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td></td>
<td>0</td>
<td>4</td>
<td>80000034</td>
<td>54BD</td>
<td>V6E--R-</td>
<td>----B</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td></td>
<td>0</td>
<td>2</td>
<td>80000044</td>
<td>95A5</td>
<td>V6E--R-</td>
<td>----B</td>
</tr>
</tbody>
</table>

Network Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Adv Router</th>
<th>Link Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Csum</th>
<th>Options</th>
<th>Rtr</th>
<th>Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>636</td>
<td>636</td>
<td>80000001</td>
<td>8B0D</td>
<td>V6E--R-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Inter Network States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Adv Router</th>
<th>Link Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Csum</th>
<th>Options</th>
<th>Rtr</th>
<th>Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>1</td>
<td>323</td>
<td>80000001</td>
<td>3970</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>1</td>
<td>322</td>
<td>80000001</td>
<td>1B8A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>2</td>
<td>293</td>
<td>80000001</td>
<td>3529</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>2</td>
<td>375</td>
<td>80000001</td>
<td>FC5E</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Adv Router</th>
<th>Link Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Csum</th>
<th>Options</th>
<th>Rtr</th>
<th>Opt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>634</td>
<td>700</td>
<td>80000008</td>
<td>2D89</td>
<td>V6E--R-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>634</td>
<td>689</td>
<td>80000000A</td>
<td>6F82</td>
<td>V6E--R-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>635</td>
<td>590</td>
<td>80000001</td>
<td>7782</td>
<td>V6E--R-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Intra Prefix States (Area 0.0.0.0)

Layer 3 Routing Commands | 1800
### show ipv6 ospf database database-summary

Use the `show ipv6 ospf database database-summary` command to display the number of each type of LSA in the database and the total number of LSAs in the database.

#### Syntax

```
show ipv6 ospf database database-summary
```

#### Default Configuration

This command has no default configuration.
**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the number of each type of LSA in the database and the total number of LSAs in the database.

```
console#show ipv6 ospf database database-summary
OSPF Router with ID (0.0.0.2)
Router database summary
Router......................................... 0
Network........................................ 0
Inter-area Prefix............................ 0
Inter-area Router............................ 0
Type-7 Ext..................................... 0
Link........................................... 0
Intra-area Prefix............................ 0
Link Unknown................................... 0
Area Unknown................................... 0
AS Unknown.................................... 0
Type-5 Ext..................................... 0
Self-Originated Type-5 Ext................... 0
Total.......................................... 0
```

**show ipv6 ospf interface**

Use the `show ipv6 ospf interface` command to display the information for the IFO object or virtual interface tables.

**Syntax**

```
show ipv6 ospf interface [interface-type interface-number]
```

- **interface-type**—The interface type, VLAN, tunnel or loopback
- **interface-number**—The valid interface number, a valid VLAN ID, tunnel identifier (Range: 0–7) or loopback identifier (Range: 0–7).

**Default Configuration**

This command has no default configuration.
**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the information in VLAN 11’s virtual interface tables.

```
console#show ipv6 ospf interface vlan 11
IP Address................................. 11.11.11.11
ifIndex.................................... 1
OSPF Admin Mode.......................... Enable
OSPF Area ID............................... 0.0.0.0
Router Priority........................... 1
Retransmit Interval....................... 5
Hello Interval............................ 10
Dead Interval.............................. 40
LSA Ack Interval......................... 1
Iftransit Delay Interval................ 1
Authentication Type...................... None
Metric Cost.................................. 10 (computed)
OSPF Mtu-ignore........................... Disable
OSPF cannot be initialized on this interface.
```

**show ipv6 ospf interface brief**

Use the `show ipv6 ospf interface brief` command to display brief information for the IFO object or virtual interface tables.

**Syntax**

`show ipv6 ospf interface brief`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
The following example displays brief ospf interface information.

```console
show ipv6 ospf interface brief
```

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Router</td>
<td>Hello</td>
<td>Dead</td>
<td>Retrax</td>
<td>LSA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use the `show ipv6 ospf interface stats` command to display the statistics for a specific interface. The command only displays information if OSPF is enabled.

Syntax
show ipv6 ospf interface stats vlan vlan-id
- vlan-id — Valid VLAN ID.

Default Configuration
This command has no default configuration.

Command Mode
User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the interface statistics for VLAN 5.

```console
show ipv6 ospf interface stats vlan 5
OSPfv3 Area ID............................... 0.0.0.1
Spf Runs........................... 265
```
Area Border Router Count....................... 1
AS Border Router Count.......................... 0
Area LSA Count.................................. 6
IPv6 Address..................................
FE80::202:BCFF:FE00:3146/1283FFE::2/64
OSPF Interface Events........................... 53
Virtual Events.................................... 13
Neighbor Events.................................. 6
External LSA Count................................ 0
LSAs Received.................................... 660
Originate New LSAs................................. 853
Sent Packets...................................... 1013
Received Packets................................ 893
Discards.......................................... 48
Bad Version....................................... 0
Virtual Link Not Found............................ 9
Area Mismatch..................................... 39
Invalid Destination Address....................... 0
No Neighbor at Source Address..................... 0
Invalid OSPF Packet Type......................... 0

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>295</td>
<td>219</td>
</tr>
<tr>
<td>Database Description</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>LS Request</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>LS Update</td>
<td>521</td>
<td>398</td>
</tr>
<tr>
<td>LS Acknowledgment</td>
<td>209</td>
<td>282</td>
</tr>
</tbody>
</table>

show ipv6 ospf interface vlan

Use the `show ipv6 ospf interface vlan` command to display OSPFv3 configuration and status information for a specific VLAN.

**Syntax**

`show ipv6 ospf interface vlan {vlan-id | brief}`

- vlan-id — Valid VLAN ID. Range is 1-4093.
- brief — Displays a snapshot of configured interfaces.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines

This command has no user guidelines.

Example

The following example displays OSPF interface VLAN information.

```
console#show ipv6 ospf interface vlan 10
IPv6 Address............................. FE80::2FC:E3FF:FE90:44
ifIndex.................................. 634
OSPF Admin Mode......................... Enable
OSPF Area ID.................................. 0.0.0.1
Router Priority.......................... 1
Retransmit Interval...................... 5
Hello Interval........................... 10
Dead Interval............................ 40
LSA Ack Interval........................ 1
Iftransit Delay Interval................. 1
Authentication Type...................... None
Metric Cost................................ 10 (computed)
OSPF Mtu-ignore.......................... Disable
OSPF Interface Type...................... broadcast
State.................................... backup-designated-router
Designated Router...................... 1.1.1.1
Backup Designated Router.............. 2.2.2.2
Number of Link Events................... 46
```
Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Examples
The following examples display information about OSPF neighbors, in the first case in a summary table, and in the second in a table specific to tunnel 1.

```
console#show ipv6 ospf neighbor
Router ID Priority Intf Interface    State         Dead
ID                              Time
--------- -------- ---- -----------  ------------- ----

console#show ipv6 ospf neighbor interface tunnel 1
IP Address.................................... 2.4.6.8
ifIndex........................................ 619
OSPF Admin Mode.............................. Enable
OSPF Area ID.................................. 0.0.0.0
Router Priority.............................. 1
Retransmit Interval.......................... 5
Hello Interval................................ 10
Dead Interval.................................. 40
LSA Ack Interval.............................. 1
Iftransit Delay Interval..................... 1
Authentication Type.......................... None
Metric Cost.................................... 1 (computed)
OSPF Mtu-ignore.............................. Disable
OSPF cannot be initialized on this interface.
```

show ipv6 ospf range
Use the `show ipv6 ospf range` command to display information about the area ranges for the specified area identifier.

Syntax
show ipv6 ospf range areaid
• areaid — Identifies the OSPF area whose ranges are being displayed.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays information about the area ranges for area 1.

```
console#show ipv6 ospf range 1
Area ID   IPv6 Prefix/Prefix Length  Lsdb Type       Advertisement
--------- -------------------------  --------------- --------------
```

**show ipv6 ospf stub table**
Use the show ipv6 ospf stub table command to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

**Syntax**
show ipv6 ospf stub table

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.
Example
The following example displays the OSPF stub table.

```
console#show ipv6 ospf stub table
AreaId       TypeofService   Metric Val   Import SummaryLSA
------------ -------------   ----------   -----------------
 0.0.0.10          Normal         1             Enable
```

show ipv6 ospf virtual-links
Use the show ipv6 ospf virtual-links command to display the OSPF Virtual Interface information for a specific area and neighbor or for all areas in the system.

Syntax
```
show ipv6 ospf virtual-link [area-id neighbor-id | brief]
```
- area-id — Identifies the OSPF area whose virtual interface information is being displayed.
- neighbor-id — Router ID of neighbor.

Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the OSPF Virtual Interface information for area 1 and its neighbor.

```
console#show ipv6 ospf virtual-link 1 1.1.1.1
Area ID................................. 1
Neighbor Router ID.................... 1.1.1.1
Hello Interval......................... 10
Dead Interval......................... 40
```
Iftransit Delay Interval ....................... 1
Retransmit Interval............................ 5
State.............................................. point-to-point
Metric.......................................... 10
Neighbor State................................. Full

**show ipv6 ospf virtual-link brief**

Use the `show ipv6 ospf virtual-link brief` command to display the OSPFV3 Virtual Interface information for all areas in the system.

**Syntax**

`show ipv6 ospf virtual-link brief`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the OSPF stub table.

```
console(config)#show ipv6 ospf virtual-link brief
```

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Neighbor</th>
<th>Hello Interval</th>
<th>Dead Interval</th>
<th>Retransmit Interval</th>
<th>Transit Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**timers throttle spf**

Use the `timers throttle spf` command to throttle the link-state-packets. Use the `no` form of the command to return the configured parameters to their default values.
Syntax

timers throttle spf spf-start spf-hold spf-maximum

no timers throttle spf

- spf-start—Configures the delay used when no SPF calculation has been scheduled during the current wait interval. (Range: 1–60000 milliseconds)
- spf-hold—Configures the initial wait interval. (Range: 1–60000 milliseconds)
- spf-maximum—Configures the maximum wait interval. (Range: 1–60000 milliseconds)

Default Configuration

The default value for spf-start is 2000 milliseconds.
The default value for spf-hold is 5000 milliseconds.
The default value for spf-maximum is 5000 milliseconds.

Command Mode

OSPFv3 Configuration mode.

User Guidelines

The timers throttle command throttles the generation of link-state packets (LSPs). Receipt of an LSP will initiate an SPF calculation in the router. LSP throttling reduces route flapping and the load on other OSPF routers in the network.

The initial wait interval is set to the value of spf-hold. If an SPF calculation is not initiated during the current wait interval, the next SPF calculation is scheduled spf-start milliseconds later. This wait interval is doubled on each subsequent expiry if an SPF calculation is initiated during the interval. Initiating an SPF calculation resets the wait interval to the value of spf-hold. The wait interval is not allowed to exceed the value of spf-maximum.

Command History

Command introduced in version 6.5 firmware.
Example

console(config-router6)#timers throttle spf 3000 6000 18000
Router Discovery Protocol Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

Routers can be configured to periodically send router discovery messages to announce their presence to locally attached hosts. The router discovery message advertises one or more IP addresses on the router that hosts can use as their default gateway. Hosts can send a router solicitation message asking any router that receives the message to immediately send a router advertisement, so that the host does not have to wait for the next periodic message.

Router discovery enables hosts to select from among multiple default gateways and switch to a different default gateway if an initially designated gateway goes down.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>ip irdp multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip irdp holdtime</td>
<td>ip irdp preference</td>
</tr>
<tr>
<td>ip irdp maxadvertinterval</td>
<td>show ip irdp</td>
</tr>
<tr>
<td>ip irdp minadvertinterval</td>
<td>–</td>
</tr>
</tbody>
</table>

ip irdp

Use the ip irdp command in Interface Configuration mode to enable Router Discovery on an interface. Use the no form of the command to disable Router Discovery.

Syntax

```
ip irdp [multicast | holdtime seconds | maxadvertinterval seconds | minadvertinterval seconds | preference number | address address]
no ip irdp holdtime
```
- **multicast**—Configure the address that the interface uses to send the router discovery advertisements to be 224.0.0.1, the all-hosts IP multicast address. Use the `no` form of the command to use 255.255.255.255, the limited broadcast address.
- **holdtime** seconds—Integer value in seconds of the holdtime field of the router advertisement sent from this interface. (Range: 4-9000 seconds)
- **maxadvertinterval** seconds—Maximum time in seconds allowed between sending router advertisements from the interface. (Range: 4 or the minimum advertisement interval, whichever is greater, and 1800 seconds).
- **minadvertinterval** seconds—Minimum time in seconds allowed between sending router advertisements from the interface. (Range: 3 to value of maximum advertisement interval in seconds)
- **preference** number—Preference of the address as a default router address, relative to other router addresses on the same subnet. (Range: -2147483648 to 2147483647)
- **address** address—IP address for router discovery advertisements. (Range: 224.0.0.1 [all-hosts IP multicast address] or 255.255.255.255 [limited broadcast address])

**Default Configuration**
- Router discovery is disabled by default.
- 1800 seconds is the default value for holdtime.
- 600 seconds is the default value for maxadvertinterval.
- The minadvertinterval default value is 450.
- The preference default value is 0.
- IP address 224.0.0.1 is the default configuration for address.

**Command Mode**
Interface Configuration (VLAN) mode

**User Guidelines**
This command has no user guidelines.
Example

The following example enables router discovery on the selected interface.

```bash
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp
```

**ip irdp holdtime**

Use the `ip irdp holdtime` command in Interface Configuration mode to configure the value, in seconds, of the holdtime field of the router advertisement sent from this interface. Use the no form of the command to set the time to the default value.

**Syntax**

```
ip irdp holdtime integer
no ip irdp holdtime
```

- `integer` — Integer value in seconds of the holdtime field of the router advertisement sent from this interface. The holdtime must be no less than the maximum advertisement interval and cannot be greater than 9000 seconds.

**Default Configuration**

The holdtime defaults to 3 times the maximum advertisement interval.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

The holdtime is the length of time that a host considers the router advertisement valid. After the holdtime expires, a host will no longer use the router as its default gateway.

**Example**

The following example sets hold time at 2000 seconds for VLAN 15.

```bash
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp holdtime 2000
```
ip irdp maxadvertinterval

Use the `ip irdp maxadvertinterval` command in Interface Configuration mode to configure the maximum time, in seconds, allowed between sending router advertisements from the interface. Use the `no` form of the command to set the time to the default value.

**Syntax**

```plaintext
ip irdp maxadvertinterval integer
no ip irdp maxadvertinterval
```

- `integer` — Maximum time in seconds allowed between sending router advertisements from the interface. (Range: 4 or the minimum advertisement interval, whichever is greater, and 1800 seconds)

**Default Configuration**

600 seconds is the default value.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

The default values of the minimum advertisement interval and the holdtime depend on the value of the maximum advertisement interval. Setting the maximum advertisement interval changes the minimum advertisement interval and holdtime if those values are at their defaults; so, the maximum advertisement interval should always be set first. If the minimum advertisement interval has been configured to a non-default value, the maximum advertisement interval cannot be configured to a lower value than the minimum advertisement interval. If the holdtime has been configured to a non-default value, the maximum advertisement interval cannot be configured to a value larger than the holdtime.

**Example**

The following example sets maximum advertisement interval at 600 seconds for VLAN 15.

```plaintext
console(config)#interface vlan 15
```
ip irdp minadvertinterval

Use the ip irdp minadvertinterval command in Interface Configuration mode to configure the minimum time, in seconds, allowed between sending router advertisements from the interface. Use the no form of the command to set the time to the default value.

Syntax

ip irdp minadvertinterval integer
no ip irdp minadvertinterval

• integer — Minimum time in seconds allowed between sending router advertisements from the interface. (Range: 3 to value of maximum advertisement interval in seconds)

Default Configuration

The default value is 0.75 times the maximum advertisement interval.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets minimum advertisement interval at 100 seconds for VLAN 15.

console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp minadvertinterval 100
ip irdp multicast

To send router advertisements as IP multicast packets, use the `ip irdp multicast` command in Interface Configuration mode. To send router advertisements to the limited broadcast address (255.255.255.255), use the no form of this command.

**Syntax**

```
ip irdp multicast
no ip irdp multicast
```

**Default Configuration**

Router discovery packets are sent to the all hosts IP multicast address (224.0.0.1) by default.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

If a subnet includes any hosts that do not accept IP multicast packets, send router advertisements to the limited broadcast address.

**Example**

The following example configures router discovery to send to the limited broadcast address:

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp multicast
```

**ip irdp preference**

Use the `ip irdp preference` command in Interface Configuration mode to configure the preference of the address as a default router address relative to other router addresses on the same subnet. Use the no form of the command to set the preference to the default value.
Syntax

ip irdp preference integer

no ip irdp preference

- integer — Preference of the address as a default router address, relative to other router addresses on the same subnet. (Range: -2147483648 to 2147483647)

Default Configuration

0 is the default value.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the ip irdp preference to 1000 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp preference 1000
```

show ip irdp

Use the `show ip irdp` command to display the router discovery information for all interfaces, or for a specified interface.

Syntax

```
show ip irdp [vlan vlan-id ]
```

- vlan-id — Valid VLAN ID

Default Configuration

This command has no default configuration.
**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example shows router discovery information for VLAN 15.

```console
console#show ip irdp vlan 15
Interface   Ad Mode  Advertise Address Max Int Min Int Hold Time Preference
----------  -------  ----------------- ------- ------- -------- ----------
vlan15      Enable  224.0.0.1            600     450     1800       0
```
Routing Information Protocol
Commands

Dell EMC Networking N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

The Routing Information Protocol (RIP) has been a long-standing protocol used by routers for exchanging route information. RIP is a distance vector protocol whereby each route is characterized by the number of gateways, or hops, a packet must traverse to reach its intended destination. Categorized as an interior gateway protocol, RIP operates within the scope of an autonomous system. RIP is a simple protocol. Its usefulness is limited to moderately sized networks whose physical interconnections are of similar type and speed.

Dell EMC Networking routing supports RIPv2 as specified in RFC 2453.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>auto-summary</th>
<th>host routes accept</th>
<th>router rip</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-information</td>
<td>ip rip</td>
<td>show ip rip</td>
</tr>
<tr>
<td>originate (Router RIP Configuration)</td>
<td>ip rip authentication</td>
<td>show ip rip interface</td>
</tr>
<tr>
<td>default-metric</td>
<td>ip rip receive version</td>
<td>show ip rip interface brief</td>
</tr>
<tr>
<td>distance rip</td>
<td>ip rip send version</td>
<td>split-horizon</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>redistribute (RIP)</td>
<td>–</td>
</tr>
</tbody>
</table>

auto-summary

Use the auto-summary command in Router RIP Configuration mode to enable the RIP auto-summearization mode. Use the no form of the command to disable auto-summearization mode.
Syntax
auto-summary
no auto-summary

Default Configuration
Disabled is the default configuration.

Command Mode
Router RIP Configuration mode.

User Guidelines
This command has no user guidelines.

Example
console(config-router)#auto-summary

default-information originate (Router RIP Configuration)
Use the default-information originate command in Router RIP Configuration mode to control the advertisement of default routes.

Syntax
default-information originate
no default-information originate

Default Configuration
The default configuration is no default-information originate.

Command Mode
Router RIP Configuration mode.
**User Guidelines**

Only routers that actually have Internet connectivity should advertise a default route. All other routers in the network should learn the default route from routers that have connections out to the Internet.

**Example**

```
console(config-router)#default-information originate
```

**default-metric**

Use the `default-metric` command in Router RIP Configuration mode to set a default for the metric of distributed routes. Use the `no` form of the command to return the metric to the default value.

**Syntax**

```
default-metric number-value
no default-metric
```

- `number-value` — Metric for the distributed routes. (Range: 1-15)

**Default Configuration**

Default metric is not configured by default.

**Command Mode**

Router RIP Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example sets a default of 12 for the metric of distributed routes.

```
console(config-router)#default-metric 12
```
distance rip

Use the distance rip command in Router RIP Configuration mode to set the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. Use the no form of the command to return the preference to the default value.

Syntax

distance rip integer

no distance rip

• integer — RIP route preference. (Range: 1-255)

Default Configuration

15 is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the route preference value of RIP in the router at 100.

console(config-router)#distance rip 100

distribute-list out

Use the distribute-list out command in Router RIP Configuration mode to specify the access list to filter routes received from the source protocol. Use the no form of the command to remove the access list from the specified source protocol.

Syntax

distribute-list accesslistname out {bgp | ospf | static | connected}
no distribute-list accesslistname out {bgp | ospf | static | connected}
  - accesslistname — The name used to identify the existing ACL. The range is 1-31 characters.
  - bgp — Apply the specified access list when BGP is the source protocol.
  - ospf — Apply the specified access list when OSPF is the source protocol.
  - static — Apply the specified access list when packets come through a static route.
  - connected — Apply the specified access list when packets come from a directly connected route.

Default Configuration
This command has no default configuration.

Command Mode
Router RIP Configuration mode.

User Guidelines
The access list has an implicit deny all, so it is advisable to have a permit statement somewhere on the access list.
The BGP parameter is only available in firmware versions enabled for BGP.

Example
The following example elects access list ACL40 to filter routes received from the source protocol.

console(config-router)#distribute-list ACL40 out static

enable
Use the enable command in Router RIP Configuration mode to reset the default administrative mode of RIP in the router (active). Use the no form of the command to disable the administrative mode for RIP.

Syntax
enable
no enable

**Default Configuration**

Enabled is the default configuration.

**Command Mode**

Router RIP Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-router)#enable
```

**hostroutesaccept**

Use the `hostroutesaccept` command in Router RIP Configuration mode to enable the RIP hostroutesaccept mode. Use the no form of the command to disable the RIP hostroutesaccept mode.

**Syntax**

```
hostroutesaccept
no hostroutesaccept
```

**Default Configuration**

Enabled is the default configuration.

**Command Mode**

Router RIP Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-router)#hostroutesaccept
```
ip rip

Use the `ip rip` command in Interface Configuration mode to enable RIP on a router interface. Use the no form of the command to disable RIP on the interface.

**Syntax**

```
ip rip
no ip rip
```

**Default Configuration**

Disabled is the default configuration.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-if-vlan2)#ip rip
console(config-if-vlan2)#no ip rip
```

ip rip authentication

Use the `ip rip authentication` command in Interface Configuration Mode to set the RIP Version 2 Authentication Type and Key for the specified VLAN. Use the no form of the command to return the authentication to the default value.

**Syntax**

```
ip rip authentication {none | {simple key} | {encrypt key key-id}}
no ip rip authentication
```

- none—Do not use RIP authentication on the VLAN.
- simple—Use simple authentication on the VLAN.
- key — Authentication key for the VLAN. (Range: 16 bytes or less)
• encrypt — Use MD5 encryption for the RIP interface.
• key-id — Authentication key identifier for authentication type encrypt. (Range: 0-255)

Default Configuration
This command has no default configuration.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets the RIP Version 2 Authentication Type and Key for VLAN 11.

console(config-if-vlan11)#ip rip authentication encrypt pass123 35

ip rip receive version
Use the ip rip receive version command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version(s) to be received. Use the no form of the command to return the version to the default value.

Syntax
ip rip receive version {rip1 | rip2 | both | none}
no ip rip receive version
• rip1 — Receive only RIP version 1 formatted packets.
• rip2 — Receive only RIP version 2 formatted packets.
• both — Receive packets from either format.
• none — Do not allow any RIP control packets to be received.
Default Configuration
Both is the default configuration.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
This command has no user guidelines.

Example
The following example allows no RIP control packets to be received by VLAN 11.

```
console(config-if-vlan11)#ip rip receive version none
```

**ip rip send version**

Use the `ip rip send version` command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version to be sent. Use the no form of the command to return the version to the default value.

**Syntax**

```
ip rip send version {rip1 | rip1c | rip2 | none}
```

```
no ip rip send version
```

- `rip1` — Send RIP version 1 formatted packets.
- `rip1c` — Send RIP version 1 compatibility mode, which sends RIP version 2 formatted packets via broadcast.
- `rip2` — Send RIP version 2 using multicast.
- `none` — Do not allow any RIP control packets to be sent.

Default Configuration
RIP2 is the default configuration.
**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example allows no RIP control packets to be sent by VLAN 11.

```
console(config-if-vlan11)#ip rip send version none
```

**redistribute (RIP)**

The `redistribute` command configures RIP protocol to redistribute routes from the specified sources. If the source protocol is OSPF, there are five possible match options.

**Syntax**

```
redistribute ospf [metric integer] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]]
no redistribute [ospf | bgp | static | connected]
redistribute {bgp | connected | static} [metric integer]
```

- **metric integer** — Specifies the metric to use when redistributing the route. Range: 0-15.
- **match internal** — Adds internal matches to any match types presently being redistributed.
- **match external 1** — Adds routes imported into OSPF as Type-1 external routes into any match types presently being redistributed.
- **match external 2** — Adds routes imported into OSPF as Type-2 external routes into any match types presently being redistributed.
- **match nssa-external 1** — Adds routes imported into OSPF as NSSA Type-1 external routes into any match types presently being redistributed.
- **match nssa-external 2** — Adds routes imported into OSPF as NSSA Type-2 external routes into any match types presently being redistributed.
- **static** — Redistributes static routes.
Layer 3 Routing Commands

- `bgp` — Redistributes BGP originated routes.
- `connected` — Redistributes directly-connected routes.

**Default Configuration**

`metric` integer — not configured  
`match` — internal

**Command Mode**

Router RIP Configuration mode.

**User Guidelines**

When redistributing a route metric, the receiving protocol must understand the metric. The OSPF metric is a cost value equal to \(10^8/\text{link bandwidth in bits/sec}\). For example, the OSPF cost of GigabitEthernet is \(1 = 10^8/10^8 = 1\).

The RIP metric is a hop count with a maximum value of 15.

Dell EMC Networking RIP does not support sending a tag value.

Redistribution of BGP-originated routes is only available on BGP-enabled routers. Redistribution of BGP-originated routes into RIP is not recommended.

**Example**

```
console(config-router)#redistribute ospf metric 10 match nssa-external 1  
console(config-router)#redistribute connected metric 1
```

**router rip**

Use the `router rip` command in Global Configuration mode to enter Router RIP mode.

**Syntax**

`router rip`

**Default Configuration**

RIP is globally enabled by default. RIP is not enabled on any interfaces by default.
**Command Mode**

Global Configuration mode.

**User Guidelines**

Use the `enable` and `no enable` commands in router RIP mode to enable and disable RIP globally.

**Example**

The following example enters Router RIP mode.

```sh
console(config)#router rip
console(config-router)#
```

**show ip rip**

Use the `show ip rip` command to display information relevant to the RIP router.

**Syntax**

`show ip rip`

**Default Configuration**

The command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays information relevant to the RIP router.

```sh
console#show ip rip
RIP Admin Mode................................. Enable
Split Horizon Mode.............................. Simple
Auto Summary Mode.............................. Enable
```
Host Routes Accept Mode.......................... Enable
Global route changes........................... 0
Global queries.................................... 0
Default Metric................................... 12
Default Route Advertise........................ 0
Redistributing....................................
Source............................................. Connected
Metric.............................................. 2
Distribute List.................................... Not configured
Redistributing....................................
Source............................................. ospf
Metric.............................................. 10
Match Value...................................... 'nssa-external 1'
Distribute List.................................... Not configured

**show ip rip interface**

Use the *show ip rip interface* command to display information related to a particular RIP interface.

**Syntax**

```
show ip rip interface vlan vlan-id
```

- vlan-id — Valid VLAN ID.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays information related to the VLAN 15 RIP interface.

```
console#show ip rip interface vlan 15
Interface...................................... 15
IP Address..................................... -----
```
Send version................................... RIP-2
Receive version................................ Both
RIP Admin Mode................................ Disable
Link State..................................... ----- 
Authentication Type............................ MD5
Authentication Key............................ “pass123”
Authentication Key ID.......................... 35
Bad Packets Received........................... ----- 
Bad Routes Received............................. ----- 
Updates Sent................................... ----- 

**show ip rip interface brief**

Use the `show ip rip interface brief` command to display general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

**Syntax**

`show ip rip interface brief`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays general information for each RIP interface.

```
console#show ip rip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>Send Version</th>
<th>Receive Version</th>
<th>RIP Mode</th>
<th>Link State</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>0.0.0.0</td>
<td>RIP-2</td>
<td>Both</td>
<td>Disable</td>
<td>Down</td>
</tr>
<tr>
<td>vlan2</td>
<td>0.0.0.0</td>
<td>RIP-2</td>
<td>Both</td>
<td>Disable</td>
<td>Down</td>
</tr>
</tbody>
</table>
```
**split-horizon**

Use the `split-horizon` command in Router RIP Configuration mode to set the RIP split horizon mode. Use the no form of the command to return the mode to the default value.

**Syntax**

```
split-horizon {none | simple | poison}
```

```
no split-horizon
```

- **none** — RIP does not use split horizon to avoid routing loops.
- **simple** — RIP uses split horizon to avoid routing loops.
- **poison** — RIP uses split horizon with poison reverse (increases routing packet update size).

**Default Configuration**

Simple is the default configuration.

**Command Mode**

Router RIP Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example does not use split horizon.

```
console(config-router)#split-horizon none
```
Tunnel Interface Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

Dell EMC Networking provides for the creation, deletion, and management of tunnel interfaces. They are dynamic interfaces that are created and deleted by user configuration.

Tunnel interfaces are used for the following purposes.

- IPv4 tunnels
- IPv6 tunnels

Each router interface (port or VLAN interface) may have associated tunnel interfaces. Each interface can have multiple tunnel interfaces. There is no set limit to the number of tunnel interfaces associated with a router interface. There is a compile platform limitation to the number of tunnel interfaces available to the entire system.

To support IPv4 to IPv6 transition, Dell EMC Networking supports configured tunnels (RFC 4213) and automatic 6to4 tunnels (RFC 3056). 6to4 tunnels are automatically formed for IPv4 tunnels carrying IPv6 traffic. The automatic tunnels IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel’s next hop. Dell EMC Networking can act as a 6to4 border router that connects a 6to4 site to a 6to4 domain. The border router sends and receives tunneled traffic from routers in the 6to4 domain that include other 6to4 border routers and 6to4 relay routers.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel</td>
<td>tunnel mode ipv6ip</td>
</tr>
<tr>
<td>show interfaces tunnel</td>
<td>tunnel source</td>
</tr>
<tr>
<td>tunnel destination</td>
<td></td>
</tr>
</tbody>
</table>

interface tunnel

Use the `interface tunnel` command in Global Configuration mode to enter the interface configuration mode for a tunnel.
**Syntax**

interface tunnel tunnel-id

no interface tunnel tunnel-id

• tunnel-id — Tunnel identifier. (Range: 0–7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example enables the interface configuration mode for tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#
```

**show interfaces tunnel**

Use the `show interfaces tunnel` command to display the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

**Syntax**

show interfaces tunnel [tunnel-id]

• tunnel-id — Tunnel identifier. (Range: 0–7)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Examples
The following examples show the parameters related to an individual tunnel and to all tunnel interfaces.

```
console#show interfaces tunnel 1
Interface Link Status.......................... down
MTU size....................................... 1480 bytes

console#show interfaces tunnel
TunnelId    Interface     TunnelMode  SourceAddress   DestinationAddress
--------    ---------     ----------  -------------    ----------------
1           tunnel 1      IPv6OVER4   10.254.25.14    10.254.25.10
2           tunnel 2      IPv6OVER4   10.254.20.10    10.254.20.10
```

tunnel destination
Use the tunnel destination command in Interface Configuration mode to specify the destination transport address of the tunnel.

Syntax
tunnel destination ip-address
no tunnel destination

- ip-address — Valid IPv4 address.

Default Configuration
This command has no default configuration.

Command Mode
Interface Configuration (Tunnel) mode.

User Guidelines
This command has no user guidelines.

Example
The following example specifies the destination transport address of tunnel 1.
tunnel mode ipv6ip

Use the tunnel mode ipv6ip command in Interface Configuration mode to specify the mode of the tunnel.

Syntax

tunnel mode ipv6ip [6to4]

no tunnel mode

- 6to4 — Sets the tunnel mode to automatic.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode.

User Guidelines

This command has no user guidelines.

Example

The following example specifies ipv6ip mode for tunnel 1.

console(config)#interface tunnel 1
console(config-if-tunnell)#tunnel destination 10.1.1.1

tunnel source

Use the tunnel source command in Interface Configuration mode to specify the source transport address of the tunnel, either explicitly or by reference to an interface.

Syntax

tunnel source {ip-address | interface-type interface-number}
no tunnel source

- ip-address—Valid IPv4 address.
- interface-type—Valid interface type. VLAN is the only type supported.
- interface-number—Valid interface number.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (Tunnel) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example specifies VLAN 11 as the source transport address of the tunnel.

```plaintext
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel source vlan 11
```
Virtual Router Commands

Dell EMC Networking N3000/N3100/N4000 Series Switches

Dell EMC Networking VRF is an implementation of Virtual Routing and Forwarding (VRF). Virtual Routing and Forwarding allows multiple independent instances for the forwarding plane to exist simultaneously. This allows the administrator to segment the network without incurring the costs of multiple routers. Each VRF operates as an independent VPN. The IP addresses assigned to each VPN may overlap. Static route leaking to and from the global instance is supported. VRF associated VLANs may not overlap with other VRF instances.

The following capabilities are supported for Dell EMC Networking VRFs:

- Static routing (including route leaking)
- OSPF (IPv4 only)
- ARP
- Ping
- VRRP
- Trace route
- DHCP relay (IP helper)
- ICMP echo reply configuration
- ICMP error interval configuration

VRF configuration follows the same configuration steps as the default routing instance with two additional steps: creating the VRF instance and associating VLANs to the instance. Existing commands that have been enabled for VRF accept an additional VRF instance identifier (name). VRF names can be up to 32 characters in length. If a VRF instance identifier is not used in the command, it applies to the global routing instance by default.

To create a VRF and enable OSPF routing in the VRF:

1. Create the VLAN instances associated to the VRF. It is recommended that a VLAN numbering scheme be developed to allow for future growth and to assist in the easy recognition of which VLANs are associated to which VRFs.
2. In global config mode, create the pool of VLANs.
console#configure terminal
console(config)#vlan 100-109
console(config-vlan100-109)#exit

3 Assign the VLAN to an interface.
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport access vlan 100
console(config-if-Gi1/0/1)#exit

4 Create the VRF and enable routing.
console(config)#ip vrf red
console(config-vrf-red)#ip routing
console(config-vrf-red)#exit

5 Assign IP addresses to the interfaces.
console(config)#interface vlan 100
console(config-if-vlan100)#ip address 192.168.0.1 /24

6 Put the VLAN interface into the VRF.
console(config-if-vlan100)#ip vrf forwarding red
console(config-if-vlan100)#exit

7 Routing interface moved from Default router instance to red router instance.

8 Enable OSPF on the VRF, assign a network, and enable OSPF for the VRF
console(config)#router ospf vrf red
console(Config-router-vrf-red)#network 192.168.0.0 0.0.0.255 area 0
console(Config-router-vrf-red)#router-id 192.168.0.253
console(Config-router-vrf-red)#redistribute connected
console(Config-router-vrf-red)#enable
console(Config-router-vrf-red)#exit

Commands in this Section
This section explains the following commands, which are exclusive to VRFs. Other commands such as ip routing may also be executed in VRF configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description ip vrf forwarding</td>
<td></td>
</tr>
<tr>
<td>ip vrf</td>
<td>maximum routes</td>
</tr>
<tr>
<td>–</td>
<td>show ip vrf</td>
</tr>
</tbody>
</table>
description

This optional command assigns descriptive text to the VRF instance.

**Syntax**

description text

- text—Descriptive text. Enclose the description in quotes if embedded blanks are desired.

**Default Configuration**

No descriptive text is assigned.

**Command Mode**

Virtual Router Configuration

**User Guidelines**

There are no user guidelines for this command.
Example
The following example shows the assignment of descriptive text to a VRF.

```
console(config)#ip vrf Red
console(config-vrf-Red)#description "Backbone to Gateway"
console(config-vrf-Red)#exit
```

**ip vrf**

This command creates a virtual router with a specified name and enters Virtual Router Configuration mode. If the virtual router instance already exists, it simply enter virtual router configuration mode. This command optionally reserves the number of routes allowed as well as sets the maximum limit on the number of routes for a virtual router instance, in the total routing table space for the router, provided there is enough free space in the router’s total routing table.

**Syntax**

```
ip vrf vrf-name
no ip vrf vrf-name
```

- vrf-name—The name of a VRF. The name must consist of printable ASCII characters other than a question mark and may not have leading or trailing spaces. Spaces may be included if the name is enclosed in quotes. The maximum length of a VRF name is 32 characters.

**Default Configuration**

A single global VRF is created when routing is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command is only available on the N3000/N3100/N4000 switches.

Up to 52 VRFs may be configured on the N4000 and up to 12 VRFs may be configured on the N3000 and N3100. If sufficient resources requested by the VRF instance, such as routes, are not available to create the router instance, a warning is shown and the VRF is not created.
The ARP table, among others, is a shared resource and is not allocated or partitioned on a VRF basis. Global commands such as `arp cachesize` still limit the physical router’s shared resources.

**Example**

The following example creates two virtual router instances. The routing in the virtual router instance is enabled only when the `ip routing` command is issued at the virtual router level.

```
(Console) (Config)#ip vrf Red
(Console) (Config-vrf-Red)#ip routing
(Console) (Config-vrf-Red)#exit
(Console) (Config)#ip vrf Blue
(Console) (Config-vrf-Blue)#ip routing
(Console) (Config-vrf-Blue)#exit
```

**ip vrf forwarding**

This command associates an interface with a VRF instance. Use the `no` form of the command to associate the interface with the global routing table.

**Syntax**

- `ip vrf forwarding vrf-name`
- `no ip vrf forwarding`
  - `vrf-name`—The name of the VRF with which to associate the interface.

**Default Configuration**

All interfaces are members of the global routing instance.

**Command Mode**

Interface (VLAN) Configuration mode, Interface Range (VLAN) Configuration mode, Interface (Loopback) Configuration mode

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

This command is only available on the N3000/N3100/N4000 switches.
L3 configuration on an interface, including the IP address, is retained when the interface migrated to a new VRF instance. A interface may be migrated from the global routing instance to a VRF or from any non-global VRF instances as well.

**Example**

The following example shows the configuration of two VRFs (Red and Blue) for IPv4 routing. Both VRFs will operate over two trunk ports (te1/0/1-2) on their respective VLANs (100 and 200).

```
console(config)#ip vrf Red
console(config-vrf-Red)#ip routing
console(config-vrf-Red)#exit
console(config)#ip vrf Blue
console(config-vrf-Blue)#ip routing
console(config-vrf-Blue)#exit
console(config)#vlan 100,200
console(config-vlan100,200)#exit
console(config)#interface range te1/0/1-2
console(config-if)#switchport mode trunk
console(config-if)#exit
console(config)#interface vlan 100
console(config-if-vlan100)#ip vrf forwarding Red
console(config-if-vlan100)#exit
console(config)#interface vlan 200
console(config-if-vlan200)#ip vrf forwarding Blue
console(config-if-vlan200)#exit
```

**maximum routes**

This command reserves the number of routes allowed and sets the maximum limit on the number of routes for a virtual router instance in the total routing table space for the router, provided there is enough free space in the router’s total routing table.

**Syntax**

```
maximum routes {limit | warn threshold}
no maximum routes [warn]
```

- limit—Reserve this number of routes for the VRF instance.
- threshold —The percentage of total routes over which the router issues a warning that the router has allocated the specified number of routes. Range 1-100.
Default Configuration
A VRF is limited by the number of unreserved routes available.

Command Mode
Virtual Router Configuration mode

User Guidelines
Use the no maximum routes command to reset the limit to the default (unlimited).
Use the no maximum routes warn command to reset the threshold limit to the default.
A VRF instance cannot exceed the configured number of routes, nor may other VRFs utilize the resources allocated to a VRF if a limit is specified for the VRF. The maximum number of routes depends on the platform and the selected SDM template. Refer to the Platforms Constants table in the Users Configuration Guide for the maximum routes available for the selected combination of platform and SDM template. If a size larger than the total routing table size is given, the size is silently truncated to the maximum routing table size.

Example
The following example reserves 100 routes for VRF Red.
```
console(config)#ip vrf Red
console(config-vrf-Red)#ip routing
console(config-vrf-Red)#maximum routes 100
console(config-vrf-Red)#exit
```

show ip vrf
This command shows the interfaces associated with a VRF instance.

Syntax
```
show ip vrf [interfaces]
show ip vrf [vrf-name] [detail]
```
- interfaces—Displays the interfaces associated with the VRF.
• `vrf-name`—The name of the VRF for which information is displayed. If no vrf is specified, all VRFs are shown. The VRF name must match the configured VRF name exactly, including capitalization.

• `detail`—Displays detailed information regarding the VRF.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Exec mode, Privileged Exec mode, and all show modes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

If no VRF name is given, the global routing instances and all other VRF instances are shown.

This command is only available on the N3000/N3100/N4000 switches.

**Example**

```
console(config)#show ip vrf
Number of VRs........3
Name    Identifier     Route Distinguisher
--------- -------------- -------------------
Red      2              2:200
Blue     4              4:400
Green    3              3:300
console(config)#show ip vrf Red detail
VRF Identifier.................... 1
Description...................... Test network
Route Distinguisher............... 2:200
Maximum Routes.................... 512
Warning-only...................... TRUE
Route table size.................. 2
Number of interfaces............. 2

Interfaces
-----------
Vl10
Lo1
```
Export VPN route-target communities
   None

Import VPN route-target communities
   None

console(Config)#show ip vrf Red
VRF Identifier.......... 2
Description............. “India office bangalore”
Route Distinguisher..... 2:200
Maximum Routes.......... 512
Warning-only............ TRUE
Virtual Router Redundancy Protocol Commands
Dell EMC Networking N1500/N2000/N2100-ON/N3000/N3100/N4000 Series Switches

An end station running IP needs to know the address of its first hop router. While some network administrators choose to install dynamic router discovery protocols such as DHCP, others prefer to statically allocate router addresses. If the router identified by such a statically allocated address goes down, the end station loses connectivity. The Virtual Router Redundancy Protocol (VRRP) is designed to provide backup for the failing router without requiring any action on the part of the end station. It is based on the concept of having more than one router recognize the same IP address. One of the routers is elected the master router and handles all traffic sent to the specified virtual router IP address. If the master router fails, one of the backup routers is elected in its place and starts handling traffic sent to the address. This change is transparent to end stations.

VRRP increases the availability of the default path without requiring configuration of dynamic routing or router discovery protocols on every end station.

Multiple virtual routers can be defined on a single router interface.

Pingable VRRP Interface
RFC 3768 specifies that a router may only accept IP packets sent to the virtual router’s IP address if the router is the address owner. In practice, this restriction makes it more difficult to troubleshoot network connectivity problems. When a host cannot communicate, it is common to ping (send an ICMP Echo Request) the host’s default gateway to determine whether the problem is in the first hop of the path to the destination. When the default gateway is a virtual router that does not respond to pings, the operator cannot use this troubleshooting technique. Because of this, it has been common for VRRP implementations to respond to pings, in spite of the prohibition in the RFC. The IETF has recognized the issue, and a draft revision of the VRRP
RFC defines a new configuration option that allows the router to accept any packet sent to a VRRP address, regardless of whether the VRRP Master is the address owner.

The Pingable VRRP Interface feature, when enabled, allows the VRRP master to respond to both fragmented and unfragmented ICMP echo requests packets destined to a VRRP address (or addresses). A virtual router in backup state discards these. For any packet destined to a VRRP address (or addresses), the VRRP master responds with VRRP address as the source IPv4 address and VRMAC as the source MAC address. A configuration option controls whether the router responds to Echo Requests sent to a VRRP IP address.

Dell EMC Networking firmware includes a separate configuration option that controls whether the router responds to ICMP Echo Requests. When Echo Replies are disabled using that option, the VRRP master does not respond to Echo Requests, even if this new option is enabled.

**VRRP Route/Interface Tracking**

The VRRP Route/Interface Tracking feature extends the capability of the Virtual Router Redundancy Protocol (VRRP) to allow tracking of specific route/interface IP states, within the router, that can alter the priority level of a virtual router for a VRRP group. Exception to this is, if that VRRP group is the IP address owner, and, in that case, its priority is fixed at 255 and cannot be reduced through the tracking process.

VRRP Route/Interface Tracking provides a way to ensure the best VRRP router is master for the group by altering VRRP priorities to the status of tracked objects, such as IP interface or IP route states. In the process of altering the VRRP priorities the priority must not go below 1 or above the configured priority.

- **NOTE:** Note that the mastership only switches on a priority change if preempt is enabled.
Interface Tracking

For interface tracking, VRRP is a routing event client. When a routing interface goes up or down (or routing is disabled globally, implying all routing interfaces are down), VRRP checks if the interface is tracked. If so, it adjusts the priority. Interface tracking is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked.

Route Tracking

The network operator may perform this task to track the reachability of an IP route. A tracked route is considered up when a routing table entry exists for the route and the route is accessible. For route tracking, make VRRP a best route client of RTO. When a tracked route is added or deleted, change the priority. For simplicity, routes are not distinguished with the next hop interface that has VRRP enabled. So VRRP Route Tracking can ignore route modifications.

Commands in this Section

This section explains the following commands:

Virtual Router Redundancy Protocol Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip vrrp</td>
<td>vrrp timers advertise</td>
</tr>
<tr>
<td>vrrp accept-mode</td>
<td>vrrp timers learn</td>
</tr>
<tr>
<td>vrrp authentication</td>
<td>vrrp track interface</td>
</tr>
<tr>
<td>vrrp description</td>
<td>vrrp track ip route</td>
</tr>
<tr>
<td>vrrp ip</td>
<td>show vrrp</td>
</tr>
<tr>
<td>vrrp mode</td>
<td>show vrrp interface</td>
</tr>
<tr>
<td>vrrp preempt</td>
<td>–</td>
</tr>
<tr>
<td>vrrp priority</td>
<td>–</td>
</tr>
</tbody>
</table>
Virtual Router Redundancy Protocol Commands

**ip vrrp**

Use the *ip vrrp* command in Global Configuration mode to enable the administrative mode of VRRP for the router. Use the *no* form of the command to disable the administrative mode of VRRP for the router.

**Syntax**

```
ip vrrp
no ip vrrp
```

**Default Configuration**

VRRP is disabled by default.

**Command Mode**

Global Configuration mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example enables VRRP protocol on the router.

```
console(config)#ip vrrp
```

**vrrp accept-mode**

Use the *vrrp accept-mode* command in Interface (VLAN) Configuration mode to enable the VRRP Master to accept ping packets sent to one of the virtual router’s IP addresses from an external device. Use the *no* form of the command to disable responding to ping packets.

**Syntax**

```
vrrp vrid accept-mode
no vrrp vrid accept-mode
```
• vrid — Virtual router identification. (Range: 1-255)

Default Configuration
The default configuration is disabled.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
The VRRP IP address is not pingable from within the switch.

vrrp authentication
Use the vrrp authentication command in Interface Configuration mode to set the authentication details value for the virtual router configured on a specified interface. Use the no form of the command to return the authentication type to the default value.

Syntax
vrrp group authentication {none | simple key}
no vrrp group authentication

• group—The virtual router identifier. (Range: 1-255)
• none—Indicates authentication type is none.
• simple—Authentication type is a simple text password.
• key—The key for simple authentication. (Range: String values)

Default Configuration
None is the default configuration.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
This command has no user guidelines.
Example
The following example sets the authorization details value for VRRP router group 5 on VLAN 15.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#vrrp 2 authentication simple test123
```

vrrp description

Use the `vrrp description` command in Interface Configuration mode to assign a description to the Virtual Router Redundancy Protocol (VRRP) group. To remove the description, use the `no` form of the command.

**Syntax**

```
vrrp group description text
no vrrp group description
```

- **group**—The virtual router identifier. (Range: 1-255)
- **text**—Description for the virtual router group up to 80 characters.

**Default Configuration**

No description is present.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command accepts any printable characters for the name other than a question mark. Descriptions containing spaces must be enclosed in quotes.

**Example**

The following example creates virtual router group 5 on VLAN 15 and configures its description.

```console
console(config)#interface vlan 15
console(config-if-vlan15)#vrrp 5
consloe(config-if-vlan15)#vrrp 5 description “Sales and Marketing”
```
**vrrp ip**

Use the `vrrp ip` command in Interface Configuration mode to enable VRRP and set the virtual router IP address value for an interface. Use the `no` form of the command remove the secondary IP address. It is not possible to remove the primary IP address once assigned. Remove the VRRP group instead.

**Syntax**

```
vrrp group ip ip-address [secondary]
no vrrp group ip ip-address vlan secondary
```

- `group`—The virtual router identifier. (Range: 1-255)
- `ip-address`—The IP address of the virtual router.
- `secondary`—Designates the virtual router IP address as a secondary IP address on an interface.

**Default Configuration**

VRRP is not configured on the interface.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

The virtual router IP addresses must be a valid host address on the local subnet based on the IP address and subnet mask configured on the VLAN interface. The VRRP IP address cannot be either the broadcast address or a network address. To configure vrrp, perform the following steps:

1. Enable ip routing in global configuration mode.
2. Enable ip vrrp globally.
3. Set an IP address on the desired interface where VRRP is to be configured.
4. Configure the VRRP group ID on the selected interface.
5. Set the virtual router ID and address on the selected interface.
6. Enable VRRP on the interface using the `vrrp mode` command.
Example

The following example configures VRRP on VLAN 15.

```
console#configure
console(config)#vlan 15
console(config-vlan)#interface vlan 15
console(config-if-vlan15)#ip address 192.168.5.1 255.255.255.0
console(config-if-vlan15)#vrrp 20
console(config-if-vlan15)#vrrp 20 ip 192.168.5.1
console(config-if-vlan15)#vrrp 20 mode
console(config)#ip routing
console(config)#ip vrrp
```

vrrp mode

Use the `vrrp mode` command in Interface Configuration mode to enable the virtual router configured on an interface. Enabling the status field starts a virtual router. Use the no form of the command to disable the virtual router.

Syntax

```
vrrp vr-id mode
no vrrp vr-id mode
```

- `vr-id` — The virtual router identifier. (Range: 1-255)

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables the virtual router for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#vrrp 5 mode
```
vrrp preempt

Use the **vrrp preempt** command in Interface Configuration mode to set the preemption mode value for the virtual router configured on a specified interface. Use the **no** form of the command to disable preemption mode.

**Syntax**

```
vrrp group preempt [delay seconds]
no vrrp group preempt
```

- **group**—The virtual router identifier. (Range: 1-255)
- **seconds**—The number of seconds the VRRP router will wait before issuing an advertisement claiming master ownership.

**Default Configuration**

Enabled is the default configuration. Delay defaults to 0 seconds.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

As per the VRRP RFC, when preemption is enabled, the backup router discards the advertisements until the masterdowntimer starts. This feature requires immediate sending of advertisements when the preemption case occurs and the delay is 0. This is a violation according to the RFC 3768. Delay, if configured, will cause the VRRP router to wait the specified number of seconds before issuing an advertisement claiming master ownership.

**Example**

The following example sets the preemption mode value for the virtual router for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#vrrp 5 preempt
```
vrrp priority

Use the `vrrp priority` command in Interface Configuration mode to set the priority value for the virtual router configured on a specified interface. Use the `no` form of the command to return the priority to the default value.

**Syntax**

```
 vrrp group priority level
 no vrrp group priority level
```

- `group` — The virtual router identifier. (Range: 1-255)
- `level` — Priority value for the interface. (Range: 1-254)

**Default Configuration**

Priority has a default value of 100.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

The VRRP router with the highest numerical value for priority will become the VR master. When the VRRP priorities are equal, the router with the numerically highest IP address will win the election and become master. If the VRRP router is the owner of the VR IP address, its priority will be 255, and this value cannot be changed.

**Example**

The following example sets the priority value for the virtual router 5 on VLAN 15.

```
console(config-if-vlan15)#vrrp 5 priority 20
```

vrrp timers advertise

Use the `vrrp timers advertise` command in Interface Configuration mode to set the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement. Use the `no` form of the command to return the advertisement frequency to the default value.
Syntax

vrrp group timers advertise interval
no vrrp group timers advertise interval

- group — The virtual router identifier. (Range: 1-255)
- interval — The frequency at which an interface on the specified virtual router sends a virtual router advertisement. (Range: 1-255 seconds)

Default Configuration

Interval has a default value of 1.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the frequency at which the VLAN 15 virtual router 5 sends a virtual router advertisement.

console(config-if-vlan15)#vrrp 5 timers advertise 10

vrrp timers learn

Use the vrrp timers learn command in Interface Configuration mode to configure the router, when it is acting as backup virtual router for a Virtual Router Redundancy Protocol (VRRP) group, to learn the advertisement interval used by the master virtual router. Use the no form of the command to prevent the router from learning the advertisement interval from the master virtual router.

Syntax

vrrp group timers learn
no vrrp group timers learn

- group — The virtual router identifier. (Range: 1-255)
Default Configuration
Timer learning is disabled by default and the router uses the configured advertisement.

Command Mode
Interface Configuration (VLAN) mode.

User Guidelines
This command has no user guidelines.

Example
The following configures VLAN 15 virtual router to learn the advertisement interval used by the master virtual router.

```
console(config-if-vlan15)#vrrp 5 timers learn
```

vrrp track interface
Use the vrrp track interface command in Interface Configuration mode to alter the priority of the VRRP router based on the availability of its interfaces. It is useful for tracking interfaces that are not configured for VRRP. Only routing interfaces may be tracked. A tracked interface is up if routing on that interface is up. Otherwise, the tracked interface is down.

When the tracked interface is down, or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the priority argument. When the interface is up for the IP protocol, the priority will be incremented by the priority value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (default priority decrement) for each downed interface. The default priority decrement is changed using the priority argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify the interface to be tracked without giving the priority, which is optional, then the default priority will be used.
Use the **no** form of this command to remove the interface from the tracked list or to restore the priority decrement to its default. When removing an interface from the tracked list, the priority is incremented by the decrement value if that interface is down.

**Syntax**

```
vrrp group track interface vlan vlan-id [decrement priority]
no vrrp group track interface vlan vlan-id
```

- **group**—The virtual router identifier. (Range: 1-255)
- **vlan vlan-id**—Valid VLAN ID.
- **priority**—Priority decrement value for the tracked interface. (Range: 1-254)

**Default Configuration**

No interfaces are tracked. The default decrement priority is 10.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

This command has no user guidelines.

**Example**

The following example adds VLAN 2 to the virtual router tracked list (with a priority decrement value of 20.)

```
(config-if-vlan10)#vrrp 1 track interface vlan 2 decrement 20
```

**vrrp track ip route**

Use the **vrrp track ip route** command to track the route reachability. When the tracked route is deleted, the priority of the VRRP router is decremented by the value specified in the priority argument. When the tracked route is added, the priority is incremented by the same. A VRRP configured interface can track more than one route. When a tracked route goes down, the priority of the router is decreased by 10 (default priority decrement) for each downed
route. By default no routes are tracked. If we specify just the route to be tracked without specifying the optional parameter, then the default priority will be set.

Use the no form of this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, priority should be incremented by the decrement value if the route is not reachable.

**Syntax**

```plaintext
vrrp group track ip route ip-address/prefix-length [decrement priority]
no vrrp group track ip route ip-address/prefix-length
```

- **group**—The virtual router identifier. (Range: 1–255).
- **ip-address/prefix-length**—Specifies the route to be tracked.
- **priority**—Priority decrement value for the tracked route. (Range: 1–254).

**Default Configuration**

There are no routes tracked by default. The default decrement priority is 10.

**Command Mode**

Interface Configuration (VLAN) mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following example adds the route 2.2.2.0/24 to the virtual router tracked list (with a priority decrement value of 20).

```
console(config-if-vlan10)#vrrp 1 track ip route 2.2.2.0/24 decrement 20
```

**show vrrp**

Use the show vrrp command in User Exec or Privileged Exec mode to display the global VRRP configuration and status as well as the brief or detailed status of one or all VRRP groups.
**Syntax**

```show vrrp [brief | group]```

- **group**—The virtual router group identifier. Range 1-255.
- **brief**—Provide a summary view of the VRRP group information.

**Default Configuration**

Show information on all VRRP groups.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays detailed VRRP status.

```
console# show vrrp

Admin Mode..................................... Enable
Router Checksum Errors......................... 0
Router Version Errors.......................... 0
Router VRID Errors............................. 0

Vlan 7 – Group 1
Primary IP Address............................. 192.168.5.55
VMAC Address.................................. 0000.5E00.0101
Authentication Type........................... None
Priority........................................ 60
Configured Priority............................ 100
Advertisement Interval (secs).................. 10
Accept Mode.................................... Enable
Pre-empt Mode.................................. Enable
Pre-empt Delay.................................. Enable
Administrative Mode............................ Enable
State............................................. Initialized
Timers Learn Mode............................. Enable
Description....................................
Track Interface................................. vlan 3
Track Interface State........................... Down
Track Interface DecrementPriority ............. 20
Track Route (pfx/len) ......................... 10.10.10.0/24
```
Track Route Reachable ......................... False
Track Route DecrementPriority ................. 20

Vlan 7 - Group 2
Primary IP Address............................. 192.168.5.65
VMAC Address................................... 0000.5E00.0202
Authentication Type................................ None
Priority....................................... 60
Configured Priority............................ 100
Advertisement Interval (secs).................. 10
Accept Mode ................................... Enable
Pre-empt Mode................................. Enable
Pre-empt Delay.................................. 0
Administrative Mode............................ Enable
State.......................................... Initialized
Timers Learn Mode............................ Disable
Description....................................
Track Interface................................ vlan 3
Track Interface State ......................... Down
Track Interface DecrementPriority ............. 20
Track Route (pfx/len) ......................... 10.10.10.0/24
Track Route Reachable ......................... False
Track Route DecrementPriority ................. 20

console#show vrrp brief
Interface Grp Prio IP Address     Mode    State
--------- --- ---- -------------- ------  ------------
V1 1     2    60 0.0.0.0        Disable Initialize
V1 2     5    70 192.168.5.55   Enable  Initialize

show vrrp interface

Use the show vrrp interface command in User Exec or Privileged Exec mode to display all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Syntax

show vrrp interface {brief | vlan vlan-id [stats]}

- `brief`—Display summary information about each virtual router configured on the switch.
- `stats`—Display the statistical information about each virtual router configured on the VLAN.
- `vlan-id`—Display information about each virtual router configured on the VLAN. Valid interface type (VLAN) and interface number (vlan-id).
**Default Configuration**
Show information for each group in the specified interface.

**Command Mode**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays all configuration information about the VLAN 15 virtual router.

```
console#show vrrp interface vlan 15
Vlan 7 – Group 1
Primary IP Address........................... 192.168.5.55
VMAC Address................................. 0000.5E00.0101
Authentication Type.......................... None
Priority....................................... 100
Configured Priority........................... 100
Advertisement Interval (secs)................. 10
Accept Mode................................... Disable
Pre-empt Mode.................................. Enable
Pre-empt Delay.................................. 0
Administrative Mode........................... Enable
State........................................... Initialized
Timers Learn Mode............................ Disable
Description................................... GoodStuff
```

The following example displays all configuration information about the virtual router on the selected interface.

```
console#show vrrp interface brief
Interface VRID IP Address     Mode    State
--------- ---- -------------- ------  ------------
vlan1     2    0.0.0.0        Disable Initialize
vlan2     5    192.168.5.55   Enable  Initialize
```

The following example displays all statistical information about the VLAN 15 virtual router.

```
console#show vrrp interface vlan 15 stats
Vlan 15 - Group 5
UpTime....................................... 0 days 0 hrs 0 mins 0 secs
Protocol....................................... IP
```
State Transitioned to Master................... 0
Advertisement Received....................... 0
Advertisement Interval Errors................. 0
Authentication Failure........................ 0
IP TTL Errors................................ 0
Zero Priority Packets Received............... 0
Zero Priority Packets Sent.................... 0
Invalid Type Packets Received............... 0
Address List Errors......................... 0
Invalid Authentication Type................ 0
Authentication Type Mismatch............... 0
Packet Length Errors....................... 0
Switch Management Commands

This section of the document contains the following Utility command topics:

<table>
<thead>
<tr>
<th>Application Deployment Commands</th>
<th>DHCP Server Commands</th>
<th>RMON Commands</th>
<th>Telnet Server Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Install Commands</td>
<td>DHCPv6 Server Commands</td>
<td>Serviceability Commands</td>
<td>Time Ranges Commands</td>
</tr>
<tr>
<td>CLI Macro Commands</td>
<td>HiveAgent Commands</td>
<td>Sflow Commands</td>
<td>USB Flash Drive Commands</td>
</tr>
<tr>
<td>Clock Commands</td>
<td>IP Addressing Commands</td>
<td>SNMP Commands</td>
<td>User Interface Commands</td>
</tr>
<tr>
<td>Command Line Configuration Scripting Commands</td>
<td>Line Commands</td>
<td>SupportAssist Commands</td>
<td>Web Server Commands</td>
</tr>
<tr>
<td>Configuration and Image File Commands</td>
<td>PHY Diagnostics Commands</td>
<td>SYSLOG Commands</td>
<td>–</td>
</tr>
<tr>
<td>DHCP Client Commands</td>
<td>Power Over Ethernet Commands</td>
<td>System and Stack Management Commands</td>
<td>–</td>
</tr>
</tbody>
</table>
Application Deployment

This section contains commands to manage Dell-supplied or end-user generated applications.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application install</td>
<td>Use the application install command to install or remove an application.</td>
</tr>
<tr>
<td>application stop</td>
<td></td>
</tr>
<tr>
<td>application start</td>
<td></td>
</tr>
<tr>
<td>show application</td>
<td></td>
</tr>
</tbody>
</table>

**application install**

Use the application install command to install or remove an application.

**Syntax**

```
application install filename [start-on-boot] [auto-restart] [cpu-sharing percent] [max-megabytes max-megabytes]
```

```
no application install filename
```

- **filename** — Name of the file containing the executable or script that is started as a Linux process for the application.
- **start-on-boot** — Start the application every time the switch boots up. Takes affect on the subsequent reboot after set. Omit this keyword from the command to disable starting application at boot time.
- **auto-restart** — Automatically restart the application’s process(es) if they stop running. Omit this keyword from the command to disable automatic restart of the application.
- **cpu-sharing** — CPU share allocated to this application. Expressed as a percentage between 0 and 99. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value is used. The default is 0.
• max-megabytes — Set the maximum memory resource that the application process(es) are allowed to consume. Expressed as megabytes between 0 and 200. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value is used. The default is 0.

Default Configuration
By default, no applications are installed.

Command Mode
Global Configuration

User Guidelines
Application names may be up to 16 characters in length.
The name specified in the application-name parameter must match the filename output of the show application command exactly. Application names are case sensitive.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console(config)#no application install support-assist
This action will terminate the support-assist agent and remove it permanently from the switch. Are you sure you wish to continue (Y/N):

application start
Use the application start command to schedule an application for immediate execution on the stack master.

Syntax
application start application-name
• application-name — The name of the application as shown in the show application command output.
**Default Configuration**

By default, no applications are installed.

**Command Mode**

Privileged Exec mode

**User Guidelines**

Applications must be downloaded and installed prior to scheduling execution with the application start command.

Application names may be up to 16 characters in length.

The name specified in the application-name parameter must match the filename output of the show application command exactly. Application names are case sensitive.

**Example**

```
console#application start support-assist
```

**Command History**

Introduced in version 6.3.0.1 firmware. Example added in the 6.4 release.

**application stop**

Use the application stop command to stop an application if the application is executing on the stack master.

**Syntax**

```
application stop application-name
```

- application-name — The name of the application as shown in the show application command output.

**Default Configuration**

By default, no applications are started.

**Command Mode**

Privileged Exec mode
**User Guidelines**

Applications must be downloaded and installed prior to scheduling execution.

Application names may be up to 16 characters in length.

The name specified in the application-name parameter must match the filename output of the `show application` command exactly. Application names are case sensitive.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#application stop support-assist
This action will terminate the support-assist agent. Are you sure you wish to continue (Y/N):
```

**show application**

Use the `show application` command to display installed applications and optionally display application files.

**Syntax**

```
show application [files]
```

- **files** — Displays the files present in the application directory of the switch’s file system. These applications may or may not be installed.

**Default Configuration**

By default, no applications are present in the file system.

**Command Mode**

Global Configuration

**User Guidelines**

Applications must be downloaded and installed prior to displaying. The `show application` command displays the following information:
The `show application files` command format displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Name of the application file.</td>
</tr>
<tr>
<td>File size</td>
<td>Number of bytes the file occupies in the file system.</td>
</tr>
<tr>
<td>Directory Size</td>
<td>Number of bytes for all the files in the application directory.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
crunch(config)#show application
OpE application table contains 2 entries.

<table>
<thead>
<tr>
<th>Name</th>
<th>StartOnBoot</th>
<th>AutoRestart</th>
<th>CPU Sharing</th>
<th>Max Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist</td>
<td>Yes</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hiveagent</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Auto-Install Commands

Auto-Install provides automatic update of the image and configuration of Dell EMC Networking devices on boot up from a TFTP server as controlled by received DHCP options. It plays a critical role in the Dell EMC Networking offering of touchless or low-touch provisioning, in which configuration and imaging of a device is greatly simplified. This is highly desirable as device can be setup with minimum interaction from a skilled technician.

In Dell EMC Networking devices, Auto-Install provides for network-based auto-configuration and auto-imaging. Other aspects provide support for auto-configuration and auto-imaging from attached devices.

Auto-Install is available on Dell EMC Networking devices as per the specification listed below.

Auto-Install features in this release include:

1. Support download of image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch or stack of switches.

2. Support for automatic download of a configuration file from a TFTP server when the device is booted with no saved configuration file located in designated storage. This release extends the designated storage to USB flash drives. In previous releases, the only supported storage was the device’s embedded flash or non-volatile memory.

3. Support for automatic download of an image from a TFTP server in the following situations:
   a. When the device is booted with no saved configuration found in the designated storage areas.
   b. When the device is booted with a saved configuration that has Auto-Install enabled.

4. Support for the Auto-Install process from a TFTP server operationally enabling the DHCP client on designated management interfaces during the Auto-Install process. The end user configuration remains unchanged. Management interfaces include the out-of-band interface or routing interfaces in a saved config.
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot auto-copy-sw</td>
<td>Use the command to enable or disable Stack Firmware Synchronization. Use the no form of the command to disable Stack Firmware Synchronization.</td>
</tr>
<tr>
<td>boot host retry-count</td>
<td></td>
</tr>
<tr>
<td>boot auto-copy-sw allow-downgrade</td>
<td></td>
</tr>
<tr>
<td>boot host auto-reboot</td>
<td></td>
</tr>
<tr>
<td>boot host auto-save</td>
<td></td>
</tr>
<tr>
<td>boot host dhcp</td>
<td></td>
</tr>
<tr>
<td>show auto-copy-sw</td>
<td></td>
</tr>
<tr>
<td>show boot</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax**

- `boot auto-copy-sw`
- `no boot auto-copy-sw`

**Default Configuration**

Stack firmware synchronization is disabled by default.

**Command Mode**

- Global Config

**User Guidelines**

The configuration on the master switch controls the stack as if it is a single switch. No configuration steps need to be taken on the member switches to synchronize the firmware.
**boot auto-copy-sw allow-downgrade**

Use the `boot auto-copy-sw allow-downgrade` command to enable downgrading the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member. Use the `no` form of the command to disable downgrading the image.

**Syntax**

- `boot auto-copy-sw allow-downgrade`
- `no boot auto-copy-sw allow-downgrade`

**Default Configuration**

The default value is enabled.

**Command Mode**

Global Configuration

**User Guidelines**

The configuration on the stack master switch controls the stack as if it is a single switch. No configuration steps need to be taken on the member switches to downgrade the firmware version. Configuration migration during a downgrade is not assured. The operator should ensure that the configuration can be downgraded before allowing the downgrade to occur or otherwise take steps to reconfigure the switches.

During a downgrade, meta-data regarding the stack configuration is not migrated. For example, Ethernet ports configured as stacking ports will revert to the default Ethernet configuration during a downgrade. When this occurs, the stack will be split into individual switches, each of which must have the relevant Ethernet ports individually configured as stacking before the stack can be reconstituted.
**boot host auto-reboot**

Use the `boot host auto-reboot` command in Global Configuration mode to enable rebooting the device with no administrative intervention when a new firmware version is successfully downloaded using the Auto-Install process. Use the `no` form of this command to disable rebooting the device. Auto-install successfully downloads a new firmware version.

**Syntax**

```
boot host auto-reboot
no boot host auto-reboot
```

**Default Configuration**

The default value is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

The configuration on the master switch controls the stack as if it is a single switch. No configuration steps need to be taken on the member switches to enable rebooting the member switches after auto-install downloads a new firmware version.

**Example**

```
console#
console(config)#boot host auto-reboot
console(config)#no boot host auto-reboot
```

**boot host auto-save**

Use the `boot host auto-save` command in Global Configuration mode to enable automatically saving the downloaded configuration on the switch. Use the `no` form of this command to disable automatically saving the downloaded configuration on the switch.
Syntax
boot host auto-save
no boot host auto-save

Default Configuration
The default value is disabled.

Command Mode
Global Configuration mode

User Guidelines
A configuration file (CLI commands) may be downloaded during the Auto-Install process via DHCP configuration or via UCSB configuration. Refer to the DHCP and USB Auto-Configuration topic in the User’s Configuration Guide for more information.

Example
console#
crontab
console(config)#boot host auto-save
console(config)#no boot host auto-save

boot host dhcp

Use the boot host dhcp command in Global Configuration mode to enable Auto-Install and Auto Configuration on the switch. When a switch boots with a saved startup configuration that includes this command, the Auto-Install process is triggered. Use the no form of this command to disable Auto-Install on the next reboot if the reboot occurs with a saved startup configuration. If you give this command while the Auto-Install process is running, the Auto-Install process terminates. The Auto-Install process has an internal timer that retries failed installations for ten minutes.

Syntax
boot host dhcp
no boot host dhcp
Default Configuration
The default value is Enabled.

Command Mode
Global Configuration.

User Guidelines
This command has no user guidelines.

Example
console#
console#configure
console(config)#boot host dhcp
console(config)#no boot host dhcp

boot host retry-count
The boot host retry-count command sets the number of attempts to download a configuration. Use the no form of this command to reset the number of attempts to download a configuration to the default.

Syntax
boot host retry-count count
no boot host retry-count

- count — The number of attempts to download a configuration (Range: 1–6).

Default Configuration
The default number of configuration download attempts is 6.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines
Example
console#
console#configure
console(config)#boot host retry-count 5
console(config)#no boot host retry-count

show auto-copy-sw
Use the `show auto-copy-sw` command to display Stack Firmware Synchronization configuration status.

Syntax
show auto-copy-sw

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
The `show switch` command also displays the switch firmware synchronization status.

Example
console#show auto-copy-sw

Stack Firmware Synchronization

<table>
<thead>
<tr>
<th>Synchronization:</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap status:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Downgrade:</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

show boot
Use the `show boot` command to display the auto install configuration and the status.
Syntax
show boot

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
console#show boot
Auto-Install Mode.............................. Enabled
AutoInstall Operational Mode................... Disabled
Auto-Install State............................. AutoInstall is completed.

The host retry count value is: 6
Auto Save mode is Disabled
Auto Reboot mode is Enabled.
CLI Macro Commands

CLI Macros provides a convenient way to save and distribute common configurations. A CLI macro is a set of the CLI commands having a unique name. When a CLI macro is applied, the CLI commands contained within the macro are executed and added to the Running Configuration File. When the macro is applied to an interface, the existing configuration is not lost; the new commands are added configuration.

A CLI Macro may have keywords (variables) which are replaced by values provided when the macro is applied (up to 3 keywords per macro). Macros can be applied to specific interfaces, a range of interfaces, or the global configuration.

There are two types of Macros:

- Built-In Macros, or Default Macros – the predefined macros which cannot be changed or deleted.
- User-Defined Macros, or Custom Macros – the macros which allow the operator to bundle some prerequisites or global configurations as a macro and then apply them to one or more interfaces at a time, which can then be copied or used by other switches. Up to 50 user-defined macros are supported.

The software includes 6 built-in macros:

- profile-global, the global configuration, used to enable RSTP and loop guard.
- profile-desktop, the interface configuration, for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port.
- profile-phone, the interface configuration, used when connecting a desktop device such as a PC with an IP Phone to a switch port.
- profile-switch, the interface configuration, used when connecting an access switch and a distribution switch or between access switches.
- profile-router, the interface configuration, used when connecting the switch and a WAN router.
- profile-wireless, the interface configuration, used when connecting the switch and a wireless access point.
• profile-compellent-nas, the interface configuration, used when connecting the switch to a Dell Compellent NAS.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro name</td>
<td>Use the <strong>macro name</strong> command in Global Configuration mode to create a user-defined macro. Use the <strong>no</strong> form of the command to delete a macro.</td>
</tr>
<tr>
<td>macro apply</td>
<td></td>
</tr>
<tr>
<td>macro global apply</td>
<td></td>
</tr>
<tr>
<td>macro global trace</td>
<td></td>
</tr>
<tr>
<td>macro global description</td>
<td></td>
</tr>
<tr>
<td>show parser macro</td>
<td></td>
</tr>
</tbody>
</table>

**macro name**

Use the **macro name** command in Global Configuration mode to create a user-defined macro. Use the **no** form of the command to delete a macro.

**Syntax**

```
macro name name
no macro name name
```

- **name**—The name of the macro. A macro name can consist of any printable characters, including blanks and excluding question marks. A macro name may be up to 31 characters in length. Embed the name in quotes if a blank is desired in the name. Use the **no** form of the command to delete a macro.

**Default Configuration**

The following macros are defined by default and may not be deleted or altered:

<table>
<thead>
<tr>
<th>Macro Context</th>
<th>Name</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>profile-global</td>
<td>Set DSCP mappings and enable RSTP.</td>
</tr>
</tbody>
</table>
### Macro Context

<table>
<thead>
<tr>
<th>Macro Context</th>
<th>Name</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>profile-desktop</td>
<td>Configure port security and spanning-tree portfast for a desktop user.</td>
</tr>
<tr>
<td>interface</td>
<td>profile-phone</td>
<td>Enable an interface for the Voice VLAN service.</td>
</tr>
<tr>
<td>interface</td>
<td>profile-switch</td>
<td>Configure a trunk mode port for a switch.</td>
</tr>
<tr>
<td>interface</td>
<td>profile-router</td>
<td>Configure a trunk mode port for a router.</td>
</tr>
<tr>
<td>interface</td>
<td>profile-wireless</td>
<td>Configure a port for connection to a wireless AP.</td>
</tr>
<tr>
<td>global</td>
<td>profile-compellent-nas</td>
<td>Configure a port for connection to a Compellent NAS.</td>
</tr>
</tbody>
</table>

### Command Mode

Global Configuration mode

### User Guidelines

The predefined macros are useful in globally configuring the switch or a specific interface in the configuration context indicated. The macros contain a short series of commands with suggested settings for the switch or interface when used in a particular type of service.

Macros consist of text commands with one command per line. Enter the commands and terminate macro input mode by entering a single at sign (@) on a line by itself.

A macro may utilize up to 3 parameters. Parameters are text strings that begin with a dollar sign ($). Parameters are substituted by specifying the parameter on the command line when the macro is applied.

Macros may be applied to a specific interface, a range of interfaces, or to the global configuration. Up to 50 user-defined macros may be configured.
**macro global apply**

Use the `macro global apply` command in Global Configuration mode to apply a macro.

**Syntax**

`macro global apply macro-name [parameter value] [parameter value] [parameter value]`

- `macro-name`—The name of the macro.
- `parameter`—The name of the parameter recognized by the macro. The parameter must begin with a dollar sign ($).
- `value`—The string to be substituted within the macro for the specified parameter name.

**Default Configuration**

No parameters are substituted unless supplied on the command line.

**Command Mode**

Global Configuration mode

**User Guidelines**

Commands applied are additive in nature. That is, they do not remove existing configuration information by default.

**macro global trace**

Use the `macro global trace` command in Global Configuration mode to apply and trace a macro. The trace command will display each line of the macro as it is executed and list any errors encountered.

**Syntax**

`macro global trace macro-name [parameter value] [parameter value] [parameter value]`

- `macro-name`—The name of the macro.
- parameter—The name of the parameter recognized by the macro. The parameter must begin with a dollar sign ($).
- value—The string to be substituted within the macro for the specified parameter name.

**Default Configuration**
No parameters are substituted unless supplied on the command line.

**Command Mode**
Global Configuration mode

**User Guidelines**
The line number of the first error encountered is printed. The script is aborted after the first error.

Commands applied are additive in nature. That is, they do not remove existing configuration information by default.

**macro global description**
Use the macro global description command in Global Configuration mode to append a line to the global macro description. Use the no form of the command to clear the description.

**Syntax**
macro global description line
  - line—The macro description. All text up to the new line is included in the description.

**Default Configuration**
There is no description by default.

**Command Mode**
Global Configuration mode
User Guidelines
This command is intended to give the administrator an easy way to remember which macros have been applied globally. All text up to the new line is included in the description. The line is appended to the global description.

macro apply
Use the macro apply command in Interface Configuration mode to apply a macro.

Syntax
macro apply macro-name [parameter value] [parameter value][parameter value]

- macro-name—The name of the macro.
- parameter—The name of the parameter recognized by the macro. The parameter must begin with a dollar sign ($).
- value—The string to be substituted within the macro for the specified parameter name.

Default Configuration
No parameters are substituted unless supplied on the command line.

Command Mode
Interface Configuration mode

User Guidelines
Commands applied are additive in nature. That is, they do not remove existing configuration information by default.

macro trace
Use the macro trace command in Interface Configuration mode to apply and trace a macro. The command will display each line of the macro as it is executed and list any errors encountered.
**Syntax**

`macro trace` macro-name [parameter value] [parameter value] [parameter value]

`no macro name name`

-macro-name—The name of the macro.
- parameter—The name of the parameter recognized by the macro. The parameter must begin with a dollar sign ($).
- value—The string to be substituted within the macro for the specified parameter name.

**Default Configuration**

No parameters are substituted unless supplied on the command line.

**Command Mode**

Interface Configuration mode

**User Guidelines**

The line number of the first error encountered is printed. The script is aborted after the first error.

Commands applied are additive in nature. That is, they do not remove existing configuration information by default.

**macro description**

Use the `macro description` command in Interface Configuration mode to append a line to the macro description. Use the `no` form of the command to clear the description.

**Syntax**

`macro description line`

- line—The macro description. All text up to the new line is included in the description.
Default Configuration
There is no description by default.

Command Mode
Interface Configuration mode

User Guidelines
This command is intended to give the administrator an easy way to remember which macros have been applied to an interface. All text up to the new line is included in the description. The line is appended to the interface description.

show parser macro
Use the show parser macro command to display information about defined macros.

Syntax
show parser macro [brief | description [interface interface-id] | name macro
• brief—Shows the list of defined macros and their type.
• description—Shows the macro descriptions.
• name—Shows an individual macro, including its contents.
• macro—The name of the macro to display.
• interface-id—The interface for which to show the macro description.

Default Configuration
No parameters are substituted unless supplied on the command line.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
There are no user guidelines for this command.
Clock Commands

Real-time Clock

The Dell EMC Networking supports a real-time clock that maintains the system time across reboots. The system time is used to timestamp messages in the logging subsystem as well as for the application of time based ACLs. The administrator has the ability to configure and view the current time, time zone, and summer time settings.

The earliest date that can be configured is Jan 1, 2010.

Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) is widely used for synchronizing network resources. SNTP Version 4 is described in RFC 2030. SNTP is an adaptation of the Network Time Protocol (RFC 1305) useful for situations where the full performance of NTP is not justified. SNTP can operate in unicast mode (point-to-point) or broadcast mode (point-to-multipoint). Various NTP implementations can operate as either a client or a server. To an NTP or SNTP server, NTP and SNTP clients are indistinguishable. Likewise, to an NTP or SNTP client, NTP and SNTP servers are indistinguishable. Furthermore, any version of NTP is compatible with any other version of NTP. Dell EMC Networking SNTP implements the client side of SNTP.

Support for IPv6 address configuration is provided to the existing SNTP client. The end user can configure either an IPv4 or IPv6 address or a host name for an SNTP server among the list of servers. In unicast mode, one of the servers from the list is selected as the active server to be used for polling based on priority and configured order. The servers are treated alike independent of IPv4 or IPv6 or hostname address formats. At any given point of time, the client operates in unicast or broadcast mode. In broadcast mode, SNTP client listens on the well known multicast group address 224.0.1.1 (reserved for NTP) for server packets from IPv4 networks on port number 123. On IPv6 networks, the SNTP client listens to the link-local scoped IANA multicast address ff02::101 (reserved for SNTP) for server packets on port number 123. The client logic to handle packet contents doesn’t change with support for IPv6 networks.
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sntp configuration</td>
<td>show sntp configuration</td>
</tr>
<tr>
<td>show sntp server</td>
<td>sntp trusted-key</td>
</tr>
<tr>
<td>show sntp status</td>
<td>sntp unicast client enable</td>
</tr>
<tr>
<td>sntp authenticate</td>
<td>clock set</td>
</tr>
<tr>
<td>sntp authentication-key</td>
<td>clock timezone hours-offset</td>
</tr>
<tr>
<td>sntp broadcast client enable</td>
<td>no clock timezone</td>
</tr>
<tr>
<td>sntp client poll timer</td>
<td>clock summer-time recurring</td>
</tr>
<tr>
<td>sntp server</td>
<td>clock summer-time date</td>
</tr>
<tr>
<td>sntp source-interface</td>
<td>no clock summer-time</td>
</tr>
<tr>
<td>sntp source-interface</td>
<td>show clock</td>
</tr>
</tbody>
</table>

show sntp configuration

Use the `show sntp configuration` command to show the configuration of the Simple Network Time Protocol (SNTP).

Syntax

```
show sntp configuration
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

Loopback interfaces are not supported on the N1100-ON Series switches.
Example
The following example displays the current SNTP configuration of the device.

console#show sntp configuration

Polling interval: 64 seconds
MD5 Authentication keys:
Authentication is not required for synchronization.
Trusted keys: No trusted keys
No trusted keys.
Unicast clients: Disable

Unicast servers:

<table>
<thead>
<tr>
<th>Server</th>
<th>Key</th>
<th>Polling</th>
<th>Priority</th>
<th>Source Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.27.128.21</td>
<td>Disabled</td>
<td>Enabled</td>
<td>1</td>
<td>Loopback 1</td>
</tr>
</tbody>
</table>

show sntp server

Use the show sntp server command to display the preconfigured SNTP servers. The configured servers can be either IPv4 or IPv6 format.

Syntax
show sntp server

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Examples
console#show sntp server

Server Host Address: 2001::01
Server Type: IPv6
Server Stratum: 2
Server Reference Id: NTP Srv: 158.108.96.32
Server Mode: Server
Server Maximum Entries: 3
Server Current Entries: 2

SNTP Servers
------------

Host Address: 2001::01
Address Type: IPv6
Priority: 1
Version: 4
Port: 123
Last Update Time: Dec 22 11:10:00 2009
Last Attempt Time: Dec 22 11:10:00 2009
Last Update Status: Success
Total Unicast Requests: 955
Failed Unicast Requests: 1

Host Address: 3.north-america.pool.ntp.org
Address Type: DNS
Priority: 1
Version: 4
Port: 123
Last Update Time: Dec 22 07:30:31 2009
Last Attempt Time: Dec 22 07:32:41 2009
Last Update Status: Server Unsynchronized
Total Unicast Requests: 157
Failed Unicast Requests: 2

**show sntp status**

Use the **show sntp status** command to show the status of the Simple Network Time Protocol (SNTP).

**Syntax**

`show sntp status`

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Examples**
The following example shows the status of the SNTP.

```
console#show snntp status
Client Mode:                      Unicast
Last Update Time:                 Mar 8 18:43:56 2017
Unicast servers:
   Server          Status                 Last response
   ------------------ ---------------------- --------------------------
   pool.ntp.org     Success                18:43:56 Mar 8 2017
   23.101.187.68    Other                  00:00:00 Jan 1 1970
```

**snntp authenticate**
Use the `snntp authenticate` command in Global Configuration mode to require server authentication for received Network Time Protocol (NTP) traffic. To disable the feature, use the `no` form of this command.

**Syntax**

```
snntp authenticate
no snntp authenticate
```

**Default Configuration**
No authentication.

**Command Mode**
Global Configuration mode

**User Guidelines**
The command is relevant for both Unicast and Broadcast.
**Example**

The following example, after defining the authentication key for SNTP, grants authentication.

```console
console(config)# sntp authentication-key 8 md5 ClkKey
console(config)# sntp trusted-key 8
console(config)# sntp authenticate
```

**sntp authentication-key**

Use the `sntp authentication-key` command in Global Configuration mode to define an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the `no` form of this command.

**Syntax**

```
sntp authentication-key key-number md5 value
no sntp authentication-key number
```

- **key-number**—number (Range: 1–4294967295)
- **value**—value (Range: 1-8 characters)

**Default value**

No authentication is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Examples**

The following examples define the authentication key for SNTP.

```console
console(config)# sntp authentication-key 8 md5 04080605
console(config)# sntp trusted-key 8
console(config)# sntp authenticate
```
**sntp broadcast client enable**

Use the `sntp broadcast client enable` command in Global Configuration mode to enable a Simple Network Time Protocol (SNTP) Broadcast client. To disable an SNTP Broadcast client, use the `no` form of this command.

**Syntax**

```plaintext
sntp broadcast client enable
no sntp broadcast client enable
```

**Default Configuration**

The SNTP Broadcast client is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example enables a Simple Network Time Protocol (SNTP) Broadcast client.

```
console(config)# sntp broadcast client enable
```

**sntp client poll timer**

Use the `sntp client poll timer` command in Global Configuration mode to set the polling time for the Simple Network Time Protocol (SNTP) client. To return to the default settings, use the `no` form of this command.

**Syntax**

```plaintext
sntp client poll timer seconds
no sntp client poll timer
```

- seconds — Polling interval. (Range: 64-1024 seconds, in powers of 2, i.e., 64, 128, 256, 512 or 1024.)
**Default Configuration**

The default polling interval is 64 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

If a user enters a value which is not an exact power of two, the nearest power-of-two value is applied.

**Example**

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 1024 seconds.

```
console(config)# sntp client poll timer 1024
```

**sntp server**

Use the `sntp server` command in Global Configuration mode to configure an SNTP server address or a host name. The server address can be either an IPv4 address or an IPv6 address. Use the `no` form of this command to unconfigure an SNTP server address or a host name.

**Syntax**

```
sntp server {ip-address | ipv6-address | hostname} [priority priority][key key_id][poll]
```

```
no sntp server {ip-address | ipv6-address | hostname}
```

- **ip-address** — IP address of the server.
- **hostname** — Hostname of the server. (Range: 1-158 characters)
- **priority**—The relative priority of the SNTP server (Range 1-8).
- **poll**—Enable SNTP server polling.
- **key_id**—The index of the authentication key to send to the SNTP server (Range 1-4294967295).
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
The SNTP authentication parameter is an MD5 checksum sent to the NTP server. The key index identified in the `sntp server` command should be configured with the `sntp authentication-key` command.

Example
The following example configures the device to accept Simple Network Time Protocol (SNTP) traffic from the server at IP address 192.1.1.1.

```
console(config)# sntp server 192.1.1.1
```

`sntp source-interface`
Use the `sntp source-interface` command to select the interface from which to use the IP address in the source IP address field of transmitted SNTP packets. Use the `no` form of the command to revert to the default IP address.

Syntax
```
sntp source-interface {loopback loopback-id | vlan vlan-id}
no sntp source-interface
```

- `loopback-id` — A loopback interface identifier.
- `vlan-id` — A VLAN identifier.

Default Configuration
By default, the switch uses the assigned switch IP address as the source IP address for SNTP packets. This is either the IP address assigned to the VLAN from which the SNTP packet originates or the out-of-band interface IP address.
Switch Management Commands

1900

Command Mode
Global Configuration

User Guidelines
The source interface must have an assigned IP address (either manually or via another method such as DHCP). This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console#conf
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#sntp source-interface vlan 1

sntp trusted-key
Use the sntp trusted-key command in Global Configuration mode to authenticate the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the no form of this command.

Syntax
sntp trusted-key key-number
no sntp trusted-key key-number

• key-number — Key number of authentication key to be trusted. (Range: 1–4294967295)

Default Configuration
No keys are trusted.
**Command Mode**
Global Configuration mode

**User Guidelines**
This command is relevant for both received Unicast and Broadcast.

**Example**
The following defines SNTP trusted-key.
```
console(config)# sntp authentication-key 8 md5 ClkKey
console(config)# sntp trusted-key 8
console(config)# sntp authenticate
```

### sntp unicast client enable

Use the `sntp unicast client enable` command in Global Configuration mode to enable a client to use Simple Network Time Protocol (SNTP) predefined Unicast clients. To disable an SNTP Unicast client, use the `no` form of this command.

**Syntax**

```
sntp unicast client enable
no sntp unicast client enable
```

**Default Configuration**
The SNTP Unicast client is disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
Use the `sntp server` command to define SNTP servers.

**Examples**
The following example enables the device to use Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.
console(config)# sntp unicast client enable

**clock set**

Use the **clock set** command to manually set the system time.

**Syntax**
clock set {<hh:mm:ss> | <mm/dd/yyyy>}

**Default Configuration**
The system time is local.

**Command Mode**
Global Configuration

**User Guidelines**
It is advisable to set both the time and date.

**Examples**
console(config)#clock set 19:20:31
console(config)#clock set 04/01/2019

**clock timezone hours-offset**

Use the **clock timezone** [hours-offset] [minutes minutes-offset] [zone acronym] command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either '0' or '\\0', as appropriate.

**Syntax**
clock timezone hours-offset [minutes minutes-offset] [zone acronym]

- hours-offset — Hours difference from UTC. (Range: –12 to +13)
- minutes-offset — Minutes difference from UTC. (Range: 0–59)
- acronym — The acronym for the time zone. (Range: Up to four characters)
**Command Mode**
Global Configuration

**Default Value**
No default setting

**User Guidelines**
No specific guidelines

**Example**
crux(config)#clock timezone -5 minutes 30 zone IST

### no clock timezone

Use the **no clock timezone** command to reset the time zone settings.

**Syntax**

no clock timezone

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration

**User Guidelines**
This command has no specific user guidelines.

**Example**
crux(config)#no clock timezone
clock summer-time recurring

Use the `clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset offset] [zone acronym]` command to set the summertime offset to UTC recursively every year. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

**Syntax**

clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset offset] [zone acronym]

- week — Week of the month. (Range: 1–5, first, last)
- day — Day of the week. (Range: The first three letters by name; sun, for example.)
- month — Month. (Range: The first three letters by name; jan, for example.)
- hh:mm — Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- offset — Number of minutes to add during the summertime. (Range: 1–1440)
- acronym — The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

**Default Value**

No default setting

**Command Mode**

Global Configuration

**User Guidelines**

No specific guidelines

**Examples**

```
console(config)# clock summer-time recurring 1 sun jan 00:10 2 mon mar 10:00 offset 1 zone ABC
```
clock summer-time date

Use the `clock summer-time date` command to set the summertime offset to UTC. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

Syntax
clock summer-time date {date | month} {month | date} year hh:mm {date | month} {month | date} year hh:mm [offset offset] [zone acronym]

- **date** — Day of the month. (Range: 1–31)
- **month** — Month. (Range: The first three letters by name; jan, for example.)
- **year** — Year. (Range: 2000–2097)
- **hh:mm** — Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- **offset** — Number of minutes to add during the summertime. (Range: 1–1440)
- **acronym** — The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four upper or lower case alphabetic characters)

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration

User Guidelines
No specific guidelines

Examples
console(config)# clock summer-time date 1 Apr 2014 02:00 28 Oct 2014 02:00 offset 60 zone EST

or
no clock summer-time

Use the no clock summer-time command to reset the summertime configuration.

**Syntax**

no clock summer-time

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration

**User Guidelines**

No specific guidelines

**Example**

console(config)#no clock summer-time

show clock

Use the show clock command to display the time and date from the system clock. Use the show clock detail command to show the time zone and summertime configuration.

**Syntax**

show clock [detail]

**Default Configuration**

This command has no default configuration.
Command Mode
User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example shows the time and date only.

```
console# show clock
15:29:03 PDT(UTC-7) Jun 17 2014
Time source is SNTP
```

The following example shows the time, date, timezone, and summertime configuration.

```
console# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2014
Time source is SNTP
Time zone:
Acronym is PST
Offset is UTC-7
Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

The following example displays the time and date from the system clock

```
console>show clock
15:29:03 Jun 17 2014
Time source is SNTP
```
Command Line Configuration
Scripting Commands

The Configuration Scripting feature allows the user to generate text-formatted files representing the current system configuration. These configuration script files can be uploaded to a computer and edited, then downloaded to the system and applied to the system. This feature allows the flexibility of creating command configuration scripts that can be applied to several switches with minor or no modifications.

Commands applied from a script are additive in nature. That is, they modify, but do not automatically replace the current configuration. Any valid command can be placed in a script, including show commands.

Scripts execute in Privileged Exec mode. The script author must add a command (configure) in order to enter Global Configuration mode.

Commands in this Section

This section explains the following commands:

- **script apply**
- **script show**
- **script delete**
- **script validate**
- **script list**

### script apply

Use the **script apply** command to apply the commands in the script to the switch.

**Syntax**

```
script apply scriptname
```

- **scriptname** — Name of the script file to apply. (Range 1–31 characters)
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example applies the config.scr script to the switch.

```
console#script apply config.scr
```

**script delete**
Use the `script delete` command to delete a specified script.

**Syntax**
```
script delete {scriptname | all}
```
- `scriptname` — Script name of the file being deleted. (Range 1-31 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example deletes all scripts from the switch.

```
console#script delete all
```
**script list**

Use the `script list` command to list all scripts present on the switch as well as the remaining available space.

**Syntax**

```
script list
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays all scripts present on the switch.

```
console#script list
Configuration Script Name Size(Bytes)
--------------------------------  -----------
0 configuration script(s) found.
2048 Kbytes free.
```

**script show**

Use the `script show` command to display the contents of a script file.

**Syntax**

```
script show scriptname
```

- **scriptname** — Name of the script file to be displayed. (Range: 1-31 characters)

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the contents of the script file config.scr.

```console
console#script show config.scr
interface gigabitethernet 1/0/1
ip address 176.242.100.100 255.255.255.0
exit
```

**script validate**
Use the `script validate` command to validate a script file by parsing each line in the script file. The validate option is intended for use as a tool in script development. Validation identifies potential problems though it may not identify all problems with a given script.

**Syntax**

```
script validate scriptname
```

- scriptname — Name of the script file being validated. (Range: 1-31 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
This command has no user guidelines.
Example
The following example validates the contents of the script file config.scr.
console#script validate config.scr
Configuration and Image File Commands

File System Commands

CLI commands allow the user to show the contents of the current directory in the flash file system (dir command). These files may also be deleted from the flash using the delete command or renamed with the rename command. Also, the syntax of the copy command has been changed slightly to add additional flash targets and sources for the above commands.

Command Line Interface Scripting

The configuration scripting feature allows the user to save the current Dell EMC Networking configuration in text format. To modify the configuration script file, follow these procedures:

1. Upload the file to a personal computer.
2. Edit the file.
3. Download the file to a Dell EMC Networking switch.
4. Apply it to the Dell EMC Networking system. With this feature in place, the Dell EMC Networking administrator has the flexibility of creating configuration scripts and then applying the scripts to several devices.

Commands in this Section

This section explains the following commands:

- boot system
- clear config
- copy
- delete
- dir
- erase
- rename
- show backup-config
- show bootvar
- show running-config
- show startup-config
- write
boot system

Use the `boot system` command to specify the system image that the device loads at startup.

**Syntax**

`boot system [unit-id][active|backup]`

- **unit-id**—Unit to be used for this operation. If absent, command executes on this node.
- **active**—Boot from the currently active image.
- **backup**—Boot from the backup image.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

Use the `show bootvar` command to find out which image is the active image.

**Example**

```
console#boot system ?

<unit>                   Unit to be used for this operation. If absent, command executes on this node.
active                   Marks the given image as active for subsequent re-boots.
backup                   Marks the given image as active for subsequent re-boots.
```

```
console#show version

Machine Description............... Dell Networking Switch
System Model ID................... N4032
Machine Type..................... Dell Networking N4032
```
Serial Number..................... X00-32C-10
Manufacturer...................... 0xbc00
Burned In MAC Address............. 001E.C9F0.0039
System Object ID.................. 1.3.6.1.4.1.674.10895.3042
CPU Version....................... XLP308L
SOC Version....................... BCM56842_A1
HW Version......................... 1
CPLD Version....................... 17

<table>
<thead>
<tr>
<th>unit</th>
<th>active</th>
<th>backup</th>
<th>current-active</th>
<th>next-active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.0.0.1</td>
<td>6.0.0.0</td>
<td>6.0.0.1</td>
<td>6.0.0.1</td>
</tr>
</tbody>
</table>

clear config

Use the `clear config` command to restore the switch to the default configuration.

**Syntax**

clear config

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example restores the switch to its default configuration.

```
console#clear config
```

copy

Use the `copy` command to copy files within the switch and to upload and download files from and to the switch.
Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-url</td>
<td>The location URL or or reserved keyword of the source file being copied. (Range: 1-160 characters.)</td>
</tr>
</tbody>
</table>

List of valid source parameters for uploading from the switch:

- **backup-config**: Uploads Backup Config file.
- **active|backup**: Uploads code file.
- **log-files**: Uploads the system logs.
- **operational-log**: Uploads Operational Log file.
- **running-config**: Uploads system config file.
- **script <filename>**: Uploads Configuration Script file.
- **startup-config**: Uploads Startup Config file.
- **startup-log**: Uploads Startup Log file.
- **application filename**: Uploads a PYTHON application.
- **core-dump filename**: Uploads a Core Dump file.
- **crashlog [crashlog# | kernel crashlog# | data crashlog#] [unit unit#]**: A crash log file on the stack master or a stack member.

Valid source URLs for downloading to the switch:

- `tftp://{ipaddress | hostname}/filepath/filename`
- `scp://{user@ipaddress | hostname}/filepath/filename`
- `sftp://{user@ipaddress | hostname}/filepath/filename`
- `ftp://{user@ipaddress | hostname}/filepath/filename`
- `flash://filepath/filename`
- `usb://filepath/filename`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-url</td>
<td>The URL or reserved keyword of the destination file. (Range: 1-160 characters.</td>
</tr>
</tbody>
</table>

List of valid destination parameters for downloading to the switch:

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application [filename]</td>
<td>Download a PYTHON application.</td>
</tr>
<tr>
<td>backup-config</td>
<td>Downloads a backup config file using FTP, SFTP, or TFTP.</td>
</tr>
<tr>
<td>ca-root [index]</td>
<td>A Certificate Authority (CA) root or intermediate X.509 PEM-encoded certificate file. The contents of the source URL are copied into the CAindex.pem file on the switch. The optional index can range from 1-8. If no index is given, the certificate is placed in the CA.pem file.</td>
</tr>
<tr>
<td>client-key[index]</td>
<td>A client private key file. The contents of the source URL are copied into the clientindex.key file on the switch. The optional index can range from 1-8. If no index is specified, the private key is placed into the client.key file.</td>
</tr>
<tr>
<td>client-ssl-crt[index]</td>
<td>A client certificate file. The contents of the source URL are copied into the clientindex.pem file on the switch. The optional index can range from 1-8. If no index parameter is specified, the certificate is placed in the client.pem file.</td>
</tr>
<tr>
<td>active</td>
<td>Downloads an image file by FTP, SFTP, or TFTP.</td>
</tr>
<tr>
<td>openflow-ssl-ca-cert</td>
<td>A signed Certificate Authority (CA) root or intermediate certificate file. The contents of the source URL are copied into the of-cacert.pem file on the switch.</td>
</tr>
<tr>
<td>openflow-ssl-priv-key</td>
<td>An OpenFlow client private key file. The contents of the source URL are copied into the of-privkey.pem file on the switch.</td>
</tr>
</tbody>
</table>
The following list describes syntax keywords.

- **source-url** — The location URL or reserved keyword of the source file being copied. (Range: 1–160 characters.)
- **destination-url** — The URL or reserved keyword of the destination file. (Range: 1–160 characters.)
- **ipaddr** — The IPv4 or IPv6 address of the server.
- **hostname** — Hostname of the server. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes.
- **filepath** — The path to the file on the server or USB drive or an absolute or relative path on the switch. This is an optional parameter that should only be entered if needed.
- **filename** — The name of the file on the server or USB drive (source-url). The filename parameter is required for the tftp, ftp, scp, sftp, flash and usb destination URLs. For an application, if the optional filename parameter is given for an archive in the destination url, it must have a .tar or .tgz extension. If the destination filename is not given, the

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-url</td>
<td>openflow-ssl-cert: An OpenFlow client certificate file. The contents of the source URL are copied into the of-cert.pem file on the switch.</td>
</tr>
<tr>
<td>script</td>
<td>Downloads a configuration script by FTP, SFTP, or TFTP.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Downloads a startup configuration file using FTP or TFTP.</td>
</tr>
<tr>
<td>ias-users</td>
<td>Downloads the ias-users database file.</td>
</tr>
</tbody>
</table>

Valid destination URLs for uploading from the switch:

- tftp://{ipaddress | hostname}/filepath/filename
- ftp://<user>@<ipaddr|hostname>/<path>/<filename>
- scp://{user@ipaddress | hostname}/filepath/filename
- sftp://{user@ipaddress | hostname}/filepath/filename
- flash://filename
- usb://filepath/filename
filename is extracted from the source url. If the filename has a .tar or .tgz extension, the archive is unpacked in the user-apps directory and deleted after unpacking. If there is an error during unpacking, the file is deleted anyway. If the file name does not include a .tar or .tgz extension, it is simply copied into the user-apps directory as is.

- **username** — The user name for logging into the remote server via SSH.
- **crashlog#** — Indicates the index of the log on the local or remote unit (Range 0-4). Index 0 indicates the most recent crash log. Index 4 specifies the oldest crash log.
- **unit** — Indicates the stack unit number from which to retrieve the log. If no unit is specified, the file is copied from the stack master.
- **kernel** — Only copies the kernel crash log.
- **data** — Only copies the crash summary data.

The following table lists and describes reserved keywords.

<table>
<thead>
<tr>
<th>Reserved Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>Represents an application.</td>
</tr>
<tr>
<td>running-config</td>
<td>Represents the current running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Represents the startup configuration file.</td>
</tr>
<tr>
<td>startup-log</td>
<td>Represents the startup SYSLOG file. This can only be the source of a copy operation.</td>
</tr>
<tr>
<td>operational-log</td>
<td>Represents the operational SYSLOG file. This can only be the source of a copy operation.</td>
</tr>
<tr>
<td>script scriptname</td>
<td>Represents a CLI script file.</td>
</tr>
<tr>
<td>active</td>
<td>backup</td>
</tr>
<tr>
<td>ftp:</td>
<td>Source or destination URL for an FTP network server. The syntax for this alias is ftp://ipaddr/filepath/filename image.</td>
</tr>
</tbody>
</table>
Switch Management Commands

1920

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

When copying files from the switch, match a source URL with a destination URL. URLs may not exceed 160 characters in length, including filename, file path, hostname, ip address, user, and reserved keywords. When copying firmware onto the switch in a stacked configuration, use the `show sfs` and `show version` commands to check the status of stack firmware synchronization prior to a reboot.

When copying scripts to the switch, use the script `<filename>` target syntax. Internally, all scripts, including the startup-config and backup-config, are stored with a header. The header is added when the script is downloaded to the switch and removed when the script is uploaded from the switch. Using the `flash://<filename>` syntax as the target or source bypasses adding of the script header, ensuring that when a script is applied on the switch which was previously copied to the switch using the `flash://<filename>` syntax, a syntax error will result.

<table>
<thead>
<tr>
<th>Reserved Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tftp:</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is tftp:[/location]/directory/filename. An out-of-band IP address can be specified as described in the User Guidelines.</td>
</tr>
<tr>
<td>usb:</td>
<td>Source or destination URL for a file on a mounted USB file system.</td>
</tr>
<tr>
<td>flash:</td>
<td>Source or destination URL for the switch flash-based file system.</td>
</tr>
<tr>
<td>backup-config</td>
<td>Represents the backup configuration file.</td>
</tr>
<tr>
<td>unit</td>
<td>Indicates which unit in the stack is the target of the copy command.</td>
</tr>
</tbody>
</table>
Script download performs syntax checking of downloaded scripts. If a syntax error is detected, the user is prompted to save the file. If no error is detected, the file is saved using the target file name.

Downloaded scripts are executed from privileged exec mode and should contain a `configure` command as the first line of the script in order to enter global configuration mode.

To configure TLS to use a particular CA root certificate with a client certificate and client key for connecting to a SYSLOG server, all three of the files must have the same index as is configured for the SYSLOG server.

If a CA root certificate, client certificate, or client key file is downloaded with no index specified, it becomes the default set of certificates/key file for TLS used when connecting to any SYSLOG server not configured with an index.

CA Root certificates may be self signed or signed by a certificate authority.

Applications may be installed on the switch in the user-apps directory. To copy a single application to the switch, use the `copy <source-url> application` syntax where the source-url identifies a single file. The switch will extract the application file name from the source-url.

To copy a package of related application files to the switch, tar the files into an archive (compressed or uncompressed). The switch will unpack the tar ball in the user-apps directory, and remove the downloaded archive file.

Applications in the user-apps directory may be overwritten by the copy command to support ease of installing new versions of applications. There is no warning if a file is overwritten. Application developers must embed version information in their application file names if they wish to support multiple versions of applications on the switch.

When copying files to or from a USB stick, do not remove the USB stick during file transfer. Use the `unmount` command to cleanly detach the USB stick before physical removal. After running the `unmount` command, the USB stick must be physically removed and re-inserted before accessing again.

### Examples

#### Example – Backing up the running-config

```plaintext
console#copy running-config backup-config
This operation may take a few minutes.
Management interfaces will not be available during this time.
Are you sure you want to save? (y/n) y
```
Configuration saved!

**Example – Downloading new code to the switch**

```console
console#copy tftp://10.27.9.99/jmclendo/N4000v6.0.1.3.stk backup
```

Transfer Mode.................................. TFTP
Server IP Address............................ 10.27.9.99
Source File Path.............................. jmclendo/
Source Filename................................ N4000v6.0.1.3.stk
Data Type...................................... Code
Destination Filename.......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the duration of the transfer. Please wait...

TFTP Code transfer starting...

17128797 bytes transferred...
File contents are valid. Copying file to flash...

Attempting to send the STK file to other units in the stack...

File transfer operation completed successfully.

```console
console#show bootvar
```

Image Descriptions

- active :
- backup :

Images currently available on Flash

<table>
<thead>
<tr>
<th>unit</th>
<th>active</th>
<th>backup</th>
<th>current-active</th>
<th>next-active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.0.0.8</td>
<td>6.0.1.3</td>
<td>6.0.0.8</td>
<td>6.0.0.8</td>
</tr>
</tbody>
</table>

After the file transfer completes, use the `boot system` command to select the new image to run.
Example – Downloading and applying ias users file

```
console#copy tftp://10.131.17.104/aaa_users.txt ias-users
Transfer Mode.................................. TFTP
Server IP Address.............................. 10.131.17.104
File Path...................................... ./
File Name...................................... aaa_users.txt
Data Type...................................... IAS Users
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
```

File transfer operation completed successfully.

Validating and updating the users to the IAS users database.

Updated IAS users database successfully.

Example – Script Download

```
console#copy tftp://10.27.9.99/jmclendo/max-acl.scr script maxacl.scr
```

Example – USB copy operations

```
console#copy usb:/start-config startup-config
console#copy operational-log usb://olog.txt
console#copy usb://backup-config.txt backup-config
console#copy active usb://image1.stk
console#copy flash://crashlogs/crash.0 usb://crash.0
```

Example – Crash Log

This example copies the most recent crash log from stack unit 5 to the TFTP server located at 10.27.9.99. The crash dump is transferred to the TFTP server into subdirectory ~/jcm and is named crashlog.txt

```
console#copy core-dump 0 unit 5 tftp://10.27.9.99/jcm/crashlog.txt
```

Example – Application Install

Install a single application file named hiveagent_pr_s into the user-apps directory:

```
console#copy tftp://172.25.122.22/hiveagent_pr_s application
```

Install an application package:

On the source device (a Linux workstation is shown here), perform the following steps (aggregates hiveagent_pr hiveagent_pr_s into a compressed tar ball ha.tgz):

```
linux>tar czf ha.tgz hiveagent_pr hiveagent_pr_s

On the switch, issue the following command:

console#copy tftp://172.25.122.22/ha.tgz application

See what files are installed:

console#show application files

Open application process directory contents:

   62 SupportAssist
   53926 ah_ha.conf
   53926 ah_ha.conf_s
   74062 hiveagent
   1143002 hiveagent_pr
   1143002 hiveagent_pr_s
   10517 sa-main.pyc
   2544 saCommitUpl.pyc
   3461 saGetConfig.pyc
   4465 saGlobal.pyc
   12464 saSendChunk.pyc
   3729 saStartUpl.pyc
   8707 saSubmitTop.pyc
   16358 saUtil.pyc

Total bytes for all files = 2530225

console#dir user-apps

<table>
<thead>
<tr>
<th>Attr</th>
<th>Size(bytes)</th>
<th>Creation Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwx</td>
<td>4088</td>
<td>Jul 25 2016</td>
<td>..</td>
</tr>
<tr>
<td>-rwx</td>
<td>53926</td>
<td>May 05 2016</td>
<td>ah_ha.conf</td>
</tr>
<tr>
<td>-rw</td>
<td>8707</td>
<td>Jul 19 2016</td>
<td>saSubmitTop.pyc</td>
</tr>
<tr>
<td>-rw</td>
<td>2544</td>
<td>Jul 19 2016</td>
<td>saCommitUpl.pyc</td>
</tr>
<tr>
<td>-rw</td>
<td>16358</td>
<td>Jul 19 2016</td>
<td>saUtil.pyc</td>
</tr>
<tr>
<td>-rw</td>
<td>10517</td>
<td>Jul 19 2016</td>
<td>sa-main.pyc</td>
</tr>
<tr>
<td>-rw</td>
<td>12464</td>
<td>Jul 19 2016</td>
<td>saSendChunk.pyc</td>
</tr>
<tr>
<td>-rw</td>
<td>4465</td>
<td>Jul 19 2016</td>
<td>saGlobal.pyc</td>
</tr>
<tr>
<td>-rwx</td>
<td>74062</td>
<td>May 05 2016</td>
<td>hiveagent</td>
</tr>
<tr>
<td>-rw</td>
<td>3729</td>
<td>Jul 19 2016</td>
<td>saStartUpl.pyc</td>
</tr>
<tr>
<td>-rwx</td>
<td>1143002</td>
<td>May 05 2016</td>
<td>hiveagent_pr_s</td>
</tr>
</tbody>
</table>
Command History
Description and options revised in 6.3.5 release.

delete
Use the delete command to delete files from flash. Files cannot be deleted from the USB device.

Syntax
delete {filename | backup | backup-config | startup-config | core-dump-file}
{file-name | all}

- filename — Name of the file to be deleted.
- backup — Deletes the backup.
- backup-config — Deletes the backup configuration.
- startup-config — Deletes the startup configuration.
- core-dump-file file-name - Delete the specified core dump file
- core-dump-file all — Delete all core dump files.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode
**User Guidelines**

The file name may optionally include the path to the file, e.g., `delete crashlogs/crash.0`.

**Example**

```console
console#delete file1.scr
Delete file1.scr (Y/N)? y
```

**dir**

Use the `dir` command to print the contents of the flash file system or of a subdirectory.

**Syntax**

```
dir [subdir]
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

```console
console#dir
```

```
Attr  Size(bytes)  Creation Time         Name
drwx  2640  Feb 02 2022 00:26:43 .
drwx  0  Feb 19 2014 15:22:53 ..
-rw-  96  Jan 28 2022 23:05:45 snmpOprData.cfg
-rw-  156  Jan 01 1970 00:03:14 dh512.pem
-rw- 14363703  Jan 22 2022 03:36:08 image1
-rw- 18335232  Dec 31 2021 01:03:06 image2
-rw-  64  Oct 03 2029 01:46:00 logNvmSave.bin
-rw- 37549  Jan 01 1970 00:03:02 xacl1.scr
-rw-  245  Jan 01 1970 00:03:14 dh1024.pem
drwx  160  Dec 30 2021 03:24:26 user-apps
```
Erase

Use the `erase` command to erase the startup configuration, the backup configuration, or the backup image, or a Dell-supplied application.

Syntax

```
erase {filename | startup-config | backup | backup-config | application filename}
```

- `filename`—The name of a file on the flash drive.
- `startup-config`—Erases the contents of the startup configuration file.
- `backup`—Erase the backup image.
- `backup-config`—Erases the backup configuration.
- `application filename`—Erases a Dell-supplied application.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
This command is not supported on USB drives.

Filedescr

Use the `filedescr` command to add a description to a switch image. Use the `no` version of this command to remove the description from the filename.
**Syntax**
filedescr {active | backup} description
no filedescr {active | backup}
  • active | backup—Image file.
  • description—Block of descriptive text. (Range: 0-128 characters)

**Default Configuration**
No description is attached to the active or backup image.
Use the `show bootvar` command to display the image description.

**Command Mode**
Privileged Exec mode

**User Guidelines**
The description accepts any printable characters except a question mark.
Enclose the string in double quotes to include spaces within the description.
The surrounding quotes are not used as part of the description. The CLI does not filter illegal combinations of characters on entry and may accept entries up to the first illegal character or reject the entry entirely.

**Command History**
Updated in version 6.3.0.1 firmware.

**Example**
The following example attaches a file description to the active image.

```
console#filedescr active “backedup on 03-22-05”
```

**rename**
Use the `rename` command to rename a file present in flash.

**Syntax**
rename source dest
  • source — Source file name
• dest — Destination file name

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
Renaming the image1 or image2 files may cause the switch to not boot.

**Example**

```console
console#rename file1.scr file2.scr
```

**show backup-config**

Use the `show backup-config` command to display the contents of the backup configuration file.

**Syntax**

`show backup-config`

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**

The following example shows backup-config data.

```console
console#show backup-config
```
show bootvar

Use the `show bootvar` command in User Exec mode to display the active system image file that the device loads at startup.

**Syntax**

```
show bootvar [unit]
```

- `unit` — Unit number.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the active system image file that the device loads at startup.

```
console(config)#show bootvar
```
Image Descriptions

active:
backup:

Images currently available on Flash

<table>
<thead>
<tr>
<th>unit</th>
<th>active</th>
<th>backup</th>
<th>current-active</th>
<th>next-active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.0.0.0</td>
<td>9.25.16.57</td>
<td>6.0.0.0</td>
<td>6.0.0.0</td>
</tr>
</tbody>
</table>

**show running-config**

Use the `show running-config` command to display the contents of the currently running configuration file, including banner configuration.

**NOTE:** All non-default configurations for the Captive Portal branding images and encoded Unicode are not displayed via the standard `show running-config` command. If desired, you can view this data in the script files or by using the all mode for the `show running-config` command. In addition, please note that this non-readable data is contained and displayed at the end of the script files.

**Syntax**

`show running-config [all | interface interface-id [all] | scriptname]`

- **all**—Display or capture the complete configuration, including settings equal to the defaults.
- **interface-id**—An interface identifier (logical or Ethernet). Limits the display to the specified interface.
- **scriptname**—If the optional scriptname is provided, the output is redirected to a script file.

**NOTE:** If you issue the `show running-config` command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

**Default Configuration**

By default, the `show running-config` command displays non-default values. Default configuration values are suppressed in the output. Use the `all` parameter to display both default and non-default values.
**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

This example shows the truncated output for the configuration of interface Gi1/0/1. Since the `all` parameter is given, both the non-default and the default values are shown.

```
console#show running-config interface gi1/0/1 all

speed auto
storm-control broadcast level 5
storm-control broadcast level 5
no storm-control broadcast
storm-control multicast level 5
storm-control multicast level 5
no storm-control multicast
storm-control unicast level 5
no storm-control unicast
lacp port-priority 1
lacp timeout long
no classofservice trust
cos-queue min-bandwidth 0 0 0 0 0 0
traffic-shape 0 Kbps
no switchport voice detect auto
no ip dhcp snooping trust
no ip dhcp snooping log-invalid
no dhcp 12relay
no dhcp 12relay trust
no ip dhcp snooping limit
no ipv6 dhcp snooping trust
no ipv6 dhcp snooping log-invalid
no ipv6 dhcp snooping limit
no ip verify source
no ipv6 verify source
no ip arp inspection trust
no ip arp inspection limit
```
**show startup-config**

Use the `show startup-config` command to display the startup configuration file contents.

**Syntax**

`show startup-config`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the contents of the startup-config file.

```console
console(config)#show startup-config

!Current Configuration:
!System Description "Dell Networking N4064F, 6.1.0.1, Linux 2.6.32.9"
!System Software Version 6.1.0.1
!Cut-through mode is configured as disabled
!
configure
slot 1/0 5 ! Dell Networking N4064F
slot 1/1 8 ! Dell 10GBase-T Card
stack
member 1 4 ! N4064F
exit
interface vlan 1
exit
snmp-server engineid local 800002a203000277994433
exit
```
**write**

Use the `write` command to copy the running configuration image to the startup configuration.

**Syntax**

`write`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command is equivalent to the `copy running-config startup-config` command functionally.

**Example**

```
console#write
```
DHCP Client Commands

Dell EMC Networking switches support an embedded DHCP client. Any IP interface can use DHCP to obtain an IP address. The DHCP client can run on multiple interfaces simultaneously.

For IPv4, an IP interface can either use manually configured addresses or be enabled for DHCP. The options are mutually exclusive. When the operator enables DHCPv4 on an IP interface, all manually configured IP addresses on that interface are removed from the running configuration. When the operator configures an IP address, the system automatically releases any IPv4 address assigned by a DHCP server and disables DHCPv4 on the interface.

For IPv6, DHCP can coexist with configured addresses. The operator may enable DHCPv6 and configure IPv6 addresses on the same interface. Only a single in-band interface can be configured as a DHCPv6 client.

DHCP is disabled by default on all in-band interfaces.

The DHCP client retains an IP address even if the IP interface goes down. The client does not attempt to renew its IP address until the lease expires, regardless of changes in link state.

The operator may renew or release an IP address at any time using the new release dhcp and renew dhcp CLI commands (or web or SNMP equivalents).

When an IPv6 address is leased from a DHCP server, the address has a mask length of 128. A local route for the network is only installed if the router receives and accepts IPv6 router advertisements on the interface. Because router advertisements are not accepted on a routing interface, a leased IPv6 address on a routing interface is not necessarily useful.

Commands in this Section

This section explains the following commands:

- release dhcp
- renew dhcp
- show dhcp lease
**release dhcp**

Use the `release dhcp` command to force the DHCPv4 client to release a leased address.

**Syntax**

```
release dhcp interface-id
```

- `interface-id`—Any valid VLAN interface. See Interface Naming Conventions for interface representation.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec

**User Guidelines**

The DHCP client sends a DHCP RELEASE message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another client. The interface method does not change and will still be DHCP even after issuing this command. To lease an IP address again, issue either the `renew dhcp` interface-id command below or `ip address dhcp` (Interface Configuration) command in interface mode. If the IPv4 address on the interface was not assigned by DHCP, then the command fails and displays the following error message: Error! Interface does not have a DHCP originated address.

The release dhcp option is applicable only for IP interfaces and not for the Out-of-Band port. Use the `ip address (Out-of-Band) none` command on the Out-of-Band interface to clear a DHCP-acquired address.

**Example**

```
console#release dhcp vlan 2
```

**renew dhcp**

Use the `renew dhcp` command to force the DHCP client to immediately renew an IPv4 address lease.
**Syntax**

renew dhcp {interface-id | out-of-band}

- interface-id—Any valid IP interface. See Interface Naming Conventions for interface representation.
- out-of-band—Keyword to identify the out-of-band interface. The DHCP client renews the leased address on this interface.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec

**User Guidelines**

If the interface has a leased IPv4 address when this command is issued, the DHCP client sends a DHCP REQUEST message telling the DHCP server that it wants to continue using the IP address. If DHCP is enabled on the interface, but the interface does not currently have an IPv4 address (for example, if the address was previously released), then the DHCP client sends a DISCOVER to acquire a new address. If DHCP is not enabled on the interface, then the command fails and displays the following error message:

```
DHCP is not enabled on this interface
```

The renew dhcp option is applicable only for IP interfaces and not for the Out-of-Band port. Use the `ip address out-of-band none` command on the Out-of-Band interface to clear a DHCP-acquired address.

**Examples**

The first example is for IP interfaces.

```
closeconsole#renew dhcp vlan 2
```

The second example is for an out-of-band port.

```
closeconsole#renew dhcp out-of-band
```
**show dhcp lease**

Use the `show dhcp lease` command to display IPv4 addresses leased from a DHCP server.

**Syntax**

`show dhcp lease [interface {out-of-band | vlan vlan-id}]`

- **out-of-band**—The out-of-band interface.
- **vlan-id**—The VLAN identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command lists all IPv4 addresses currently leased from a DHCP server on an IP interface. This command only applies to IP interfaces. To see the IPv4 address leased on the out-of-band interface, use the command

```
Maximum Next Hops......................... 16 out-of-band.
```

This command output provides the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address, Subnet mask</td>
<td>The IP address and network mask leased from the DHCP server.</td>
</tr>
<tr>
<td>DHCP Lease server</td>
<td>The IPv4 address of the DHCP server that leased the address.</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv4 Client on this interface.</td>
</tr>
<tr>
<td>DHCP transaction id</td>
<td>The transaction ID of the DHCPv4 Client.</td>
</tr>
<tr>
<td>Lease</td>
<td>The duration that the IP address was leased by the server.</td>
</tr>
<tr>
<td>Renewal</td>
<td>The time when the next DHCP renew Request is scheduled to renew the leased IP address.</td>
</tr>
<tr>
<td>Rebind</td>
<td>The time when the DHCP Rebind process is scheduled.</td>
</tr>
</tbody>
</table>
## Examples

The following example shows the output from this command when the device has leased two IPv4 addresses from the DHCP server.

```
console#show dhcp lease
IP address: 10.27.22.186 on interface Vl1
Subnet mask: 255.255.252.0
  DHCP lease server: 10.27.192.22, State: 5 Bound
  DHCP transaction id: 0xc9e6803a
  Lease: 2 days 23 hrs 47 mins 24 secs
  Renewal: 1 days 11 hrs 47 mins 24 secs
  Rebind: 2 days 14 hrs 47 mins 24 secs
  Retry count: 0
```
DHCP Server Commands

Dell EMC Networking N2000/N2100/N3000/N3100/N4000 Series Switches

DHCP is based on the Bootstrap Protocol (BOOTP). It also captures the behavior of BOOTP relay agents and DHCP participants can inter operate with BOOTP participants.

The host RFC’s standardize the configuration parameters which can be supplied by the DHCP server to the client. After obtaining parameters via DHCP, a DHCP client should be able to exchange packets with any other host in the Internet. DHCP is based on a client-server model.

DHCP consists of the following components:

• A protocol for delivering host-specific configuration parameters from a DHCP server to a host.

• A mechanism for allocation of network addresses to hosts.

DHCP offers the following features and benefits:

• It supports the definition of “pools” of IP addresses that can be allocated to clients by the server. Many implementations use the term scope instead of pool.

• Configuration settings like the subnet mask, default router, DNS server, that are required to make TCP/IP work correctly can be passed to the client using DHCP.

• DHCP is supported by most TCP/IP routers this allows it to allocate an IP address according to the subnet the original request came from. This means that a single DHCP server can be used in multiple subnets and that there is no need to reconfigure a client that changed subnets.

• Addresses can be leased out for a specific duration after which they need to be explicitly renewed. This allows DHCP to reclaim expired addresses and put them back into the unallocated pool.

• Internet access cost is greatly reduced by using automatic assignment as Static IP addresses are considerably more expensive to purchase than are automatically allocated IP addresses.
• Using DHCP a centralized management policy can be implemented as the DHCP server keeps information about all the subnets. This allows a system operator to update a single server when configuration changes take place.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp pool</code></td>
<td>DNS server configuration (IP DHCP Pool Config)</td>
</tr>
<tr>
<td><code>bootfile</code></td>
<td>Domain name configuration (IP DHCP Pool Config)</td>
</tr>
<tr>
<td><code>clear ip dhcp binding</code></td>
<td>Hardware address netbios-name-server show ip dhcp binding</td>
</tr>
<tr>
<td><code>clear ip dhcp conflict</code></td>
<td>Host netbios-node-type show ip dhcp conflict</td>
</tr>
<tr>
<td><code>client-identifier</code></td>
<td>Ip dhcp bootp automatic network show ip dhcp global configuration</td>
</tr>
<tr>
<td><code>client-name</code></td>
<td>Ip dhcp conflict logging next-server show ip dhcp pool</td>
</tr>
<tr>
<td><code>default-router</code></td>
<td>Ip dhcp excluded-address option show ip dhcp server statistics</td>
</tr>
</tbody>
</table>

**ip dhcp pool**

Use the **ip dhcp pool** command in Global Configuration mode to define a DHCP address pool that can be used to supply addressing information to DHCP clients. Upon successful completion, this command puts the user into DHCP Pool Configuration mode. Use the **no** form of the command to remove an address pool definition.

**Syntax**

`ip dhcp pool [pool-name]`
no ip dhcp pool [pool-name]

- pool-name—The name of an existing or new DHCP address pool. The pool name can be up to 31 characters in length and can contain the following characters: a-z, A-Z, 0-9, , ’ , , . Enclose the entire pool name in quotes if an embedded blank is to appear in the pool name.

Default Configuration
The command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
This capability requires the DHCP service to be enabled. Enable the DHCP service using the service dhcp command. Dell EMC Networking supports dynamic, automatic, and manual address assignment. Dynamic address assignment leases an address to the client for a limited period of time. Automatic assignment assigns a permanent address to a client. Manual (static) assignment simply conveys an address assigned by the administrator to the client.

In DHCP Pool Configuration mode, the administrator can configure the address space and other parameters to be supplied to DHCP clients. By default, the DHCP server assumes that all addresses specified are available for assignment to clients. Use the ip dhcp excluded-address command in Global Configuration mode to specify addresses that should never be assigned to DHCP clients.

To configure a dynamic DHCP address pool, configure the following pool properties using the listed DHCP pool commands:

- Address pool subnet and mask – network
- Client domain name – domain-name
- Client DNS server – dns-server
- NetBIOS WINS Server – netbios-name-server
- NetBIOS Node Type – netbios-node-type
- Client default router – default-router
• Client address lease time – lease

Administrators may also configure manual bindings for clients using the host command in DHCP Pool Configuration mode. This is the most often used for DHCP clients for which the administrator wishes to reserve an ip address, for example a computer server or a printer. A DHCP pool can contain automatic or dynamic address assignments or a single static address assignment.

To configure a manual address binding, configure the pool properties using the DHCP pool commands listed below. It is only necessary to configure a DHCP client identifier or a BOOTP client MAC address for a manual binding. To configure a manual binding, the client identifier or hardware address must be specified before specifying the host address.

• DHCP client identifier – client-identifier
• BOOTP client MAC address – hardware-address
• Host address – host
• Client name (optional) – client-name

Examples

Example 1 – Manual Address Pool

    console(config)#service dhcp
    console (config)#ip dhcp pool “Printer LP32 R1-101”
    console(config-dhcp-pool)#client-identifier 00:23:12:43:23:54
    console(config-dhcp-pool)#host 10.1.1.1 255.255.255.255
    console(config-dhcp-pool)#client-name PRT_PCL_LP32_R1-101

Example 2 – Dynamic Address Pool

    console(config)#service dhcp
    console(config)#ip dhcp pool “Windows PCs”
    console(config-dhcp-pool)#network 192.168.21.0 /24
    console(config-dhcp-pool)#domain-name power-connect.com
    console(config-dhcp-pool)#dns-server 192.168.22.3 192.168.23.3
    console(config-dhcp-pool)#netbios-name-server 192.168.22.2 192.168.23.2
    console(config-dhcp-pool)#netbios-node-type h-node
    console(config-dhcp-pool)#lease 2 12
    console(config-dhcp-pool)#default-router 192.168.22.1 192.168.23.1
**bootfile**

Use the `bootfile` command in DHCP Pool Configuration mode to set the name of the image for the DHCP client to load. Use the no form of the command to remove the bootfile configuration. Use the `show ip dhcp pool` command to display pool configuration parameters.

**Syntax**

```
bootfile filename
no bootfile
```

- **filename**—The name of the file for the DHCP client to load.

**Default Configuration**

There is no default bootfile filename.

**Command Mode**

DHCP Pool Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-dhcp-pool)#bootfile ntldr
```

**clear ip dhcp binding**

Use the `clear ip dhcp binding` command to remove automatic DHCP server bindings.

**Syntax**

```
clear ip dhcp binding {ip-address | *}
```

- **ip-address**—Clear a specific binding.
- *****—Clear all automatic dhcp bindings.
Default Configuration
The command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
console#clear ip dhcp binding 1.2.3.4

clear ip dhcp conflict
Use the clear ip dhcp conflict command to remove DHCP server address conflicts. Use the show ip dhcp conflict command to display address conflicts detected by the DHCP server.

Syntax
clear ip dhcp conflict {ip-address | *}
  •  *—Clear all automatic dhcp bindings.
  •  ip-address—Clear a specific address conflict.

Default Configuration
The command has no default configuration.

Command Mode
Privileged Exec mode

User Guidelines
This command has no user guidelines.

Example
console#clear ip dhcp conflict *
client-identifier

Use the client-identifier command in DHCP Pool Configuration mode to identify a Microsoft DHCP client to be manually assigned an address. Use the no form of the command to remove the client identifier configuration.

Syntax

client-identifier unique-identifier
no client-identifier

- unique-identifier—The identifier of the Microsoft DHCP client. The client identifier is specified as 7 bytes of the form XX:XX:XX:XX:XX:XX:XX where X is a hexadecimal digit.

Default Configuration

This command has no default configuration.

Command Mode

DHCP Pool Configuration mode

User Guidelines

For Microsoft DHCP clients, the identifier consists of the media type followed by the MAC address of the client. The media type 01 indicates Ethernet media.

Use the show ip dhcp pool command to display pool configuration parameters.

Example

console(config-dhcp-pool)#host 192.168.21.34 32

client-name

Use the client-name command in DHCP Pool Configuration mode to specify the host name of a DHCP client. Use the no form of the command to remove the client name configuration.
**Syntax**

```plaintext
client-name name
no client-name
```

- name—The name of the DHCP client. The client name is specified as up to 31 printable characters.

**Default Configuration**

There is no default client name.

**Command Mode**

DHCP Pool Configuration mode

**User Guidelines**

Use the show ip dhcp pool command to display pool configuration parameters. The client name should not include the domain name as it is specified separately by the domain-name (IP DHCP Pool Config) command. It is not recommended to use embedded blanks in client names.

Question marks are not allowed in the client name. Enclose the client name in quotes if a blank appears in the name.

**Example**

```plaintext
console(config-dhcp-pool)#host 192.168.21.34 32
console(config-dhcp-pool)#client-name Line_Printer_Hallway
```

**default-router**

Use the `default-router` command in DHCP Pool Configuration mode to set the IPv4 address of one or more routers for the DHCP client to use. Use the `no` form of the command to remove the default router configuration. Use the show ip dhcp pool command to display pool configuration parameters.

**Syntax**

```plaintext
default-router {ip-address1}[ip address2]
no default-router
```
- ip-address1—The IPv4 address of the first default router for the DHCP client.
- ip-address2—The IPv4 address of the second default router for the DHCP client.

**Default Configuration**
No default router is configured.

**Command Mode**
DHCP Pool Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
```
console(config-dhcp-pool)#default-router 192.168.22.1 192.168.23.1
```

**dns-server (IP DHCP Pool Config)**
Use the `dns-server` command in IP DHCP Pool Configuration mode to set the IP DNS server address which is provided to a DHCP client by the DHCP server. DNS server address is configured for stateless server support.

**Syntax**
```
dns-server ip-address1
no dns-server
```
- ip-address1—A valid IPv4 address.

**Default Configuration**
This command has no default configuration.

**Command Mode**
IP DHCP Pool Configuration mode
**User Guidelines**
This command has no user guidelines.

**domain-name (IP DHCP Pool Config)**
Use the `domain-name` command in IP DHCP Pool Configuration mode to set the DNS domain name which is provided to a DHCP client by the DHCP server. The DNS name is an alphanumeric string up to 255 characters in length. Use the `no` form of the command to remove the domain name.

**Syntax**
```
domain-name domain
no domain-name domain
```
- domain — DHCP domain name. (Range: 1–255 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
IP DHCP Pool Configuration mode

**hardware-address**
Use the `hardware-address` command in DHCP Pool Configuration mode to specify the MAC address of a client to be manually assigned an address. Use the `no` form of the command to remove the MAC address assignment.

**Syntax**
```
hardware-address hardware-address
no hardware-address
```
- hardware-address—MAC address of the client. Either the `XXXX:XXXX:XXXX` or `XX:XX:XX:XX:XX:XX` form of MAC address may be used where X is a hexadecimal digit.
Default Configuration
There are no default MAC address manual bindings.

Command Mode
DHCP Pool Configuration mode

User Guidelines
Use the show ip dhcp pool command to display pool configuration parameters. It may be necessary to use the no host command prior to executing the no hardware-address command.

Example
console(config-dhcp-pool)#hardware-address 00:23:12:43:23:54
console(config-dhcp-pool)#host 192.168.21.131 32

host
Use the host command in DHCP Pool Configuration mode to specify a manual binding for a DHCP client host. Use the no form of the command to remove the manual binding.

Syntax
host ip-address [netmask|prefix-length]
no host
• ip-address—IPv4 address to be manually assigned to the host identified by the client identifier.
• netmask—An IPv4 address indicating the applicable bits of the address, typically 255.255.255.255.
• prefix-length—A decimal number ranging from 1-30.

Default Configuration
The default is a 1 day lease.

Command Mode
DHCP Pool Configuration mode
**User Guidelines**

Use the `client-identifier` or `hardware-address` command prior to using this command for an address pool. Use the `show ip dhcp pool` command to display pool configuration parameters.

**Example**

```
console(config-dhcp-pool)#client-identifier 00:23:12:43:23:54
console(config-dhcp-pool)#host 192.168.21.131 32
```

**ip dhcp bootp automatic**

Use the `ip dhcp bootp automatic` command in Global Configuration mode to enable automatic BOOTP address assignment. By default, BOOTP clients are not automatically assigned addresses, although they may be assigned a static address. Use the `no` form of the command to disable automatic BOOTP client address assignment. Use the `show ip dhcp global configuration` command to display the automatic address assignment configuration.

**Syntax**

```
ip dhcp bootp automatic
no ip dhcp bootp automatic
```

**Default Configuration**

Automatic BOOTP client address assignment is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#ip dhcp bootp automatic
```
ip dhcp conflict logging

Use the `ip dhcp conflict logging` command in Global Configuration mode to enable DHCP address conflict detection. Use the `no` form of the command to disable DHCP conflict logging.

**Syntax**

```
ip dhcp conflict logging
no ip dhcp conflict logging
```

**Default Configuration**

Conflict logging is enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#ip dhcp conflict logging
```

**ip dhcp excluded-address**

Use the `ip dhcp excluded-address` command in Global Configuration mode to exclude one or more DHCP addresses from automatic assignment. Use the `no` form of the command to allow automatic address assignment for the specified address or address range.

**Syntax**

```
ip dhcp excluded-address low-address {high-address}
no ip dhcp excluded-address low-address {high-address}
```

- `low-address` —An IPv4 address indicating the starting range for exclusion from automatic DHCP address assignment.
• high-address—An IPv4 address indicating the ending range for exclusion from automatic DHCP address assignment. The high-address must be numerically greater than the low-address.

**Default Configuration**

By default, no IP addresses are excluded from the lists configured by the IP DHCP pool configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#ip dhcp excluded-address 192.168.20.1 192.168.20.3
```

**ip dhcp ping packets**

Use the `ip dhcp ping packets` command in Global Configuration mode to configure the number of pings sent to detect if an address is in use prior to assigning an address from the DHCP pool. If neither ping is answered, the DHCP server presumes the address is not in use and assigns the selected IP address.

**Syntax**

```
ip dhcp ping packets {0, 2-10}
no ip dhcp ping packets
```

• count—The number of ping packets sent to detect an address in use. The default is 2 packets. Range 0, 2-10. A value of 0 turns off address detection. Use the no form of the command to return the setting to the default value.

**Default Configuration**

The command has no default configuration.
**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
console#ip dhcp ping packets 5

**lease**
Use the `lease` command in DHCP Pool Configuration mode to set the period for which a dynamically assigned DHCP address is valid. Use the `infinite` parameter to indicate that addresses are to be automatically assigned. Use the `no` form of the command to return the lease configuration to the default. Use the `show ip dhcp pool` command to display pool configuration parameters. Use the `show ip dhcp binding` command to display the expiration time of the leased IP address.

**Syntax**
```plaintext
lease {days[hours][minutes]|infinite}
no lease
```
- **days**—The number of days for the lease duration. Range 0-59. Default is 1.
- **hours**—The number of hours for the lease duration. Range 0-23. There is no default.
- **minutes**—The number of minutes for the lease duration. Range 0-59. There is no default.
- **infinite**—The lease expires in 60 days.

**Default Configuration**
The default lease is 1 day.

**Command Mode**
DHCP Pool Configuration mode
User Guidelines

The Dell EMC Networking DHCP server does not offer infinite duration DHCP leases. The maximum lease offered is 60 days, which corresponds to an “infinite” setting in the UI.

Example

The following examples sets a lease period of 1 day, 12 minutes and 59 seconds.

console(config)#ip dhcp pool asd
console(config-dhcp-pool)#network 10.0.0.0 255.0.0.0
console(config-dhcp-pool)#lease 1 12 59
console(config-dhcp-pool)#exit
console(config)#show ip dhcp pool asd

Pool: asd
Pool Type...................................... Network
Network........................................ 10.0.0.0 255.0.0.0
Lease Time..................................... 1 days 12 hrs 59 mins

netbios-name-server

Use the `netbios-name-server` command in DHCP Pool Configuration mode to configure the IPv4 address of the Windows Internet Naming Service (WINS) for a Microsoft DHCP client. Use the no form of the command to remove the NetBIOS name server configuration.

Syntax

```
netbios-name-server ip-address [ip-address2...ip-address8]
no netbios-name-server
```

- ip-address—IPv4 address

Default Configuration

There is no default name server configured.

Command Mode

DHCP Pool Configuration mode
User Guidelines

Use the `show ip dhcp pool` command to display pool configuration parameters. Up to eight name server addresses may be specified. The NetBIOS WINS information is conveyed in the Option 44 TLV of the DHCP OFFER, DHCP ACK, DHCP INFORM ACK and DHCP BOOTREPLY messages.

Example

```console
console(config-dhcp-pool)#netbios-name-server 192.168.21.1 192.168.22.1
```

**netbios-node-type**

Use the `netbios-node-type` command in DHCP Pool Configuration mode to set the NetBIOS node type for a Microsoft DHCP client. Use the `no` form of the command to remove the netbios node configuration.

**Syntax**

```plaintext
netbios-node-type type
nor netbios-node-type
```

- **type**—The NetBIOS node type can be `b-node`, `h-node`, `m-node` or `p-node`.

**Default Configuration**

There is no default NetBIOS node type configured.

**Command Mode**

DHCP Pool Configuration mode

**User Guidelines**

Use the `show ip dhcp pool` command to display pool configuration parameters. The NetBIOS node type information is conveyed in the Option 46 TLV of the DHCP OFFER, DHCP ACK, DHCP INFORM ACK and DHCP BOOTREPLY messages. Supported NetBIOS node types are:

- broadcast (b-node)
- peer-to-peer (p-node)
- mixed (m-node)
•  hybrid (h-node)

**Example**

```console
console(config-dhcp-pool)#netbios-node-type h-node
```

### network

Use the `network` command in IP DHCP Pool Configuration mode to define a pool of IPv4 addresses for distributing to clients.

**Syntax**

```
network network-number [mask | prefix-length]
```

-  `network-number`—A valid IPv4 address
-  `mask`—A valid IPv4 network mask with contiguous left-aligned bits.
-  `prefix-length`—An integer indicating the number of leftmost bits in the network-number to use as a prefix for allocating cells.

**Default Configuration**

This command has no default configuration.

**Command Mode**

IP DHCP Pool Configuration mode

### next-server

Use the `next-server` command in DHCP Pool Configuration mode to set the IPv4 address of the TFTP server to be used during auto-install. Use the `no` form of the command to remove the next server configuration.

**Syntax**

```
next-server ip-address
no next-server
```

-  `ip-address`—The IPv4 address of the TFTP server to use during auto-configuration.
**Default Configuration**
There is no default IPv4 next server configured.

**Command Mode**
DHCP Pool Configuration mode

**User Guidelines**
Use the `show ip dhcp pool` command to display pool configuration parameters. The IPv4 address is conveyed in the SIADDR field of the DHCP OFFER, DHCP ACK, DHCP INFORM ACK and DHCP BOOTREPLY messages.

**Example**
```plaintext
console(config-dhcp-pool)#next-server 192.168.21.2
```

**option**
Use the `option` command in DHCP Pool Configuration mode to supply arbitrary configuration information to a DHCP client. Use the `no` form of the command to remove the option configuration. Use the `show ip dhcp pool` command to display pool configuration parameters.

**Syntax**
```plaintext
option code {ascii string1 | hex[string1...string8] | ip[ip-address1...ip-address8]}
no option code
```

- **code**—The DHCP TLV option code.
- **ascii string1**—An ASCII character string. Strings with embedded blanks must be wholly contained in quotes.
- **hex string1**—A hexadecimal string containing the characters [0-9A-F]. The string should not begin with 0x. A hex string consists of two characters which are parsed to fill a single byte. Multiple values are separated by blanks.
- **ip-address1**—An IPv4 address in dotted decimal notation.


**Default Configuration**

There is no default option configured.

**Command Mode**

DHCP Pool Configuration mode

**User Guidelines**

The option information must match the selected option type and length. Options cannot be longer than 255 characters in length. The option information is conveyed in the TLV specified by the code parameter in the DHCP OFFER, DHCP ACK, DHCP INFORM ACK and DHCP BOOTREPLY messages.

Option 125 strings must conform to the relevant TLV format as specified in RFC 3925 beginning with a 2 byte pad filled in by the switch (option code 125 and option length), the 2 byte enterprise number, the data length and the sub-option values. For example, option 125 might be written on the command line as:

```
option 125 hex 0000.02a2.1205.1061.7574.6f69.6e73.7461.6c6c.5f68.63.70
```

which translates to:

- 0x0000 - Two byte pad filled in by switch (option-code 125 and option-len)
- 0x02A2 - Dell Vendor code 674
- 0x12 - TLV length - 18 bytes
- 0x05 - Sub-option code 5
- 0x10 - Sub-option length - 16 bytes
- 0x6175746f69.6e73.7461.6c6c.5f68.63.70 - Sub-option value “autoinstall_dhcp”

Options that accept only fixed length strings need only have the relevant data bytes specified on the command line. The switch will build the TLV and insert the specified data bytes into the option. Refer to the relevant documentation for the DHCP client to identify what information, if any, is accepted by the client in DHCP Option 125.
Table 8-1 lists the other options that can be configured and their fixed length, minimum length, and length multiple requirements. Refer to the relevant documentation for the DHCP client to identify what information, if any, is accepted by the client for the options listed below.

### Table 8-1. Option Codes and Lengths

<table>
<thead>
<tr>
<th>Option Code</th>
<th>Fixed Length</th>
<th>Minimum Length</th>
<th>Multiple Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (Time Offset)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>4 (Time Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>7 (Log Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>8 (Cookie Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>9 (LPR Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>10 (Impress Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>11 (Resource Location Server)</td>
<td>–</td>
<td>4</td>
<td>+</td>
</tr>
<tr>
<td>12 (Host Name)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>13 (Boot File Size)</td>
<td>2</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>14 (Merit File Dump)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>16 (Swap Server)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>17 (Root Path)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>18 (Extensions Path)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>19 (IP Forwarding Enable)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>20 (Non-local Source Routing)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>21 (Policy Filter)</td>
<td>–</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>22 (Max Datagram Reassembly)</td>
<td>2</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>23 (IP TTL)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>24 (Path MTU Aging)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>25 (Path MTU Plateau)</td>
<td>–</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Option Code</td>
<td>Fixed Length</td>
<td>Minimum Length</td>
<td>Multiple Of</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>26 (Interface MTU)</td>
<td>2</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>27 (Subnets are local)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>28 (Broadcast Address)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>29 (Perform Mask)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>30 (Mask Supplier)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>31 (Perform Router Discovery)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>32 (Router Solicitation Address)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>33 (Static Router Option)</td>
<td>–</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>34 (Trailer Encapsulation)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>35 (ARP Cache Timeout)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>36 (Ethernet Encapsulation)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>37 (TCP TTL)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>38 (TCP Keepalive Interval)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>39 (TCP Keepalive Garbage)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>40 (Network Information Service)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>41 (Network Information Servers)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>42 (NTP Servers)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>43 (Vendor Specific Information)</td>
<td>1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>45 (NetBIOS Datagram Distribution)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>47 (Netbois Scope)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
</tbody>
</table>
## Table 8-1. Option Codes and Lengths (continued)

<table>
<thead>
<tr>
<th>Option Code</th>
<th>Fixed Length</th>
<th>Minimum Length</th>
<th>Multiple Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>48 (X-Windows Font Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>49 (X-Windows Display Manager)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>58 (Renewal Time T1)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>59 (Rebinding Time T2)</td>
<td>4</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>60 (Vendor Class)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>64 (NIS Domain)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>65 (NIS Servers)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>66 (TFTP Server)</td>
<td>–</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>68 (Mobile IP Home Agent)</td>
<td>–</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>69 (SMTP Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>70 (POP3 Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>71 (NNTP Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>72 (WWW Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>73 (Finger Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>74 (IRC Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>75 (Streettalk Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>76 (STDA Server)</td>
<td>–</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Options 19, 20, 27, 29, 30, 31, 34, 36, and 39 only accept hex 00 or hex 01 values.

**Example**

```
console(config-dhcp-pool)#option 4 ascii "ntpservice.com "
console(config-dhcp-pool)#option 42 ip 192.168.21.1
console(config-dhcp-pool)#option 29 hex 01
console(config-dhcp-pool)#option 59 hex 00 00 10 01
console(config-dhcp-pool)#option 25 hex 01 ff
```
**service dhcp**

Use the `service dhcp` command in Global Configuration mode to enable the local IPv4 DHCP server on the switch. Use the `no` form of the command to disable the DHCPv4 service.

**Syntax**

```
service dhcp
no service dhcp
```

**Default Configuration**

The service is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**sntp**

Use the `sntp` command in DHCP Pool Configuration mode to set the IPv4 address of the NTP server to be used for time synchronization of the client. Use the `no` form of the command to remove the NTP server configuration.

**Syntax**

```
sntp ip-address
no sntp
```

- **ip-address**—The IPv4 address of the NTP server to use for time services.

**Default Configuration**

There is no default IPv4 NTP server configured.

**Command Mode**

DHCP Pool Configuration mode
User Guidelines

Use the `show ip dhcp pool` command to display pool configuration parameters. The IPv4 address of the NTP server is conveyed in the Option 42 TLV of the DHCP OFFER, DHCP ACK, DHCP INFORM ACK and DHCP BOOTREPLY messages.

Example

```console
console(config-dhcp-pool)# sntp 192.168.21.2
```

**show ip dhcp binding**

Use the `show ip dhcp binding` command to display the configured DHCP bindings.

**Syntax**

```
show ip dhcp binding [address]
```

- **address**—A valid IPv4 address

**Default Configuration**

The command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```console
console(config)# show ip dhcp binding
IP address     Hardware Address    Expires    Type   client-DUID
-------------    -----------------   ---------  -----  --------------
10.10.10.3     00:0e:c6:88:0e:98   00:23:56    Auto   00:01:01:02:03:04:05:06:00:0e:c6:88:0e:98
```

Switch Management Commands | 1964
**show ip dhcp conflict**

Use the `show ip dhcp conflict` command in User Exec mode to display DHCP address conflicts for all relevant interfaces or a specified interface. If an interface is specified, the optional statistics parameter is available to view statistics for the specified interface.

**Syntax**

```
show ip dhcp conflict [address]
```

- address—A valid IPv4 address for which the conflict information is desired.

**Default Configuration**

The command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**show ip dhcp global configuration**

Use the `show ip dhcp global configuration` command to display the DHCP global configuration.

**Syntax**

```
show ip dhcp server statistics
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example

console#show ip dhcp server statistics

show ip dhcp pool
Use the show ip dhcp pool command in User Exec or Privileged Exec mode to display the configured DHCP pool or pools. If no pool name is specified, information about all pools is displayed.

Syntax

show ip dhcp pool [all | poolname]
  • poolname—Name of the pool. (Range: 1-32 characters)

Default Configuration
This command has no default configuration.

Command Mode
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

show ip dhcp server statistics
Use the show ip dhcp server statistics command to display the DHCP server binding and message counters.

Syntax

show ip dhcp server statistics

Default Configuration
This command has no default configuration.
Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
console#show ip dhcp server statistics
Automatic Bindings............................. 100
Expired Bindings............................... 32
Malformed Bindings............................. 0

<table>
<thead>
<tr>
<th>Messages</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP DISCOVER.</td>
<td>132</td>
</tr>
<tr>
<td>DHCP REQUEST.</td>
<td>132</td>
</tr>
<tr>
<td>DHCP DECLINE.</td>
<td>0</td>
</tr>
<tr>
<td>DHCP RELEASE.</td>
<td>32</td>
</tr>
<tr>
<td>DHCP INFORM.</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP OFFER.</td>
<td>132</td>
</tr>
<tr>
<td>DHCP ACK.</td>
<td>132</td>
</tr>
<tr>
<td>DHCP NACK.</td>
<td>0</td>
</tr>
</tbody>
</table>
DHCPv6 Server Commands

Dell EMC Networking N2000/N2100/N3000/N3100/N4000 Series Switches

This section explains the following commands:

<table>
<thead>
<tr>
<th>clear ipv6 dhcp</th>
<th>service dhcp</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-server (IPv6 DHCP Pool Config)</td>
<td>show ipv6 dhcp</td>
</tr>
<tr>
<td>domain-name (IPv6 DHCP Pool Config)</td>
<td>show ipv6 dhcp binding</td>
</tr>
<tr>
<td>ipv6 dhcp pool</td>
<td>show ipv6 dhcp interface (User Exec)</td>
</tr>
<tr>
<td>ipv6 dhcp relay</td>
<td>show ipv6 dhcp interface (Privileged Exec)</td>
</tr>
<tr>
<td>ipv6 dhcp server</td>
<td>show ipv6 dhcp pool</td>
</tr>
<tr>
<td>prefix-delegation</td>
<td>show ipv6 dhcp statistics</td>
</tr>
</tbody>
</table>

**clear ipv6 dhcp**

Use the `clear ipv6 dhcp` command to clear DHCPv6 statistics for all interfaces or for a specific interface.

**Syntax**

clear ipv6 dhcp {statistics | interface vlan vlan-id statistics}

- vlan-id — Valid VLAN ID.
- statistics — Indicates statistics display if VLAN is specified.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.
Examples
The following examples clears DHCPv6 statistics for VLAN 11.

```
console#clear ipv6 dhcp interface vlan 11 statistics
```

dns-server (IPv6 DHCP Pool Config)
Use the `dns-server` command in IPv6 DHCP Pool Configuration mode to set the IPv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server. DNS server address is configured for stateless server support.

**Syntax**

dns-server ipv6-address

no dns-server ipv6-address

- ipv6-address — Valid IPv6 address.

**Default Configuration**
This command has no default configuration.

**Command Mode**
IPv6 DHCP Pool Configuration mode

**User Guidelines**
This command has no user guidelines.

domain-name (IPv6 DHCP Pool Config)
Use the `domain-name` command in IPv6 DHCP Pool Configuration mode to set the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server. DNS domain name is configured for stateless server support.

**Syntax**

domain-name domain

no domain-name domain

- domain — DHCPv6 domain name. (Range: 1–255 characters)
**Default Configuration**
This command has no default configuration.

**Command Mode**
IPv6 DHCP Pool Configuration mode

**User Guidelines**
DHCPv6 pool can have multiple number of domain names with maximum of 8.

**Example**
The following example sets the DNS domain name “test”, which is provided to a DHCPv6 client by the DHCPv6 server.
```
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#domain-name test
console(config-dhcp6s-pool)#no domain-name test
```

**ipv6 dhcp pool**
This capability requires the IPv6 DHCP service to be enabled. Use the `service dhcpv6` command to enable the DHCPv6 service. Use the `ipv6 dhcp pool` command in Global Configuration mode to enter IPv6 DHCP Pool Configuration mode. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

**Syntax**
```
ipv6 dhcp pool pool-name
no ipv6 dhcp pool pool-name
```
- pool-name — DHCPv6 pool name. (Range: 1-31 characters)

**Default Configuration**
This command has no default configuration.
**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example enters IPv6 DHCP Pool Configuration mode.

```
console(config)#service dhcpv6
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#
```

**ipv6 dhcp relay**

Use the `ipv6 dhcp relay` command in Interface Configuration mode to configure an interface for DHCPv6 relay functionality.

**Syntax**

```
ipv6 dhcp relay {destination relay-address [interface vlan vlan-id] | interface vlan vlan-id}[remote-id {duid-ifid | user-defined-string}]
```

- **destination** — Keyword that sets the relay server IPv6 address.
- **relay-address** — An IPv6 address of a DHCPv6 relay server.
- **interface** — Sets the relay server interface.
- **vlan-id** — A valid VLAN ID.
- **remote-id** {duid-ifid | user-defined-string} — The Relay Agent Information Option “remote ID” suboption to be added to relayed messages. This can either be the special keyword duid-ifid, which causes the “remote ID” to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (VLAN, Tunnel) mode
User Guidelines

The IPv6 DHCP service must be enabled to use this feature. Enable the IPv6 DHCP service using the service dhcpv6 command. If relay-address is an IPv6 global address, then relay-interface is not required. If relay-address is a link-local or multicast address, then relay-interface is required. Finally, a value for relay-address is not specified, then a value for relay-interface must be specified and the DHCPV6-ALLAGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server. An IP interface (VLAN) can be configured in DHCP relay mode or DHCP server mode. Configuring an interface in DHCP relay mode overwrites the DHCP server mode and vice-versa.

An IP interface configured in relay mode cannot be configured as a DHCP client (ip address dhcp).

Example

The following example configures VLAN 15 for DHCPv6 relay functionality.

```console
console(config)#service dhcpv6
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 dhcp relay destination 2020:1::1
```

ipv6 dhcp server

Use the ipv6 dhcp server command in Interface Configuration mode to configure DHCPv6 server functionality on an interface. For a particular interface DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Syntax

ipv6 dhcp server pool-name [rapid-commit] [preference pref-value]

- pool-name — The name of the DHCPv6 pool containing stateless and/or prefix delegation parameters
- rapid-commit — An option that allows for an abbreviated exchange between the client and server.
- pref-value — Preference value—used by clients to determine preference between multiple DHCPv6 servers. (Range: 0-4294967295)
Default Configuration

The default preference value is 20. Rapid commit is not enabled by default.

Command Mode

Interface Configuration (VLAN, Tunnel) mode

User Guidelines

This feature requires the IPv6 DHCP service. Enable the IPv6 DHCP service using the `service dhcppv6` command. The `ipv6 dhcp server` command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The rapid-commit keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the rapid-commit keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the preference keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, a message is displayed.

Example

```
console#configure
console(config)#service dhcppv6
console(config)#ipv6 dhcp pool pool1
console(config-dhcp6s-pool)#address prefix-delegation 2001::/64 00:01:32:00:32:00
console(config-dhcp6s-pool)#exit
console(config)#interface vlan 10
console(config-if-vlan10)#ipv6 dhcp server pool1
```
prefix-delegation

Use the **prefix-delegation** command in IPv6 DHCP Pool Configuration mode to define multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.

**Syntax**

```
prefix-delegation ipv6-prefix/prefix-length client-DUID [name hostname] [valid-lifetime {valid-lifetime | infinite}] [preferred-lifetime {preferred-lifetime | infinite}]
```

```
no prefix-delegation ipv6-prefix/prefix-length
```

- **prefix/prefix-length**—Delegated IPv6 prefix.
- **client-DUID**—Client DUID (e.g. 00:01:00:09:f8:79:4e:00:04:76:73:43:76').
- **hostname**—Client hostname used for logging and tracing. (Range: 0-31 characters.) The command allows spaces in the host name when specified in double quotes. For example, `console(config)#snmp-server host “host name”` is allowed.
- **valid-lifetime**—Valid lifetime for delegated prefix. (Range: 0-4294967295 seconds) or use the keyword **infinite**. Using the value 0 for the valid-lifetime sets the value to the default.
- **preferred-lifetime**—Preferred lifetime for delegated prefix. (Range: 0-4294967295 seconds) or use the keyword **infinite**. Using the value 0 for the preferred-lifetime sets the value to the default.

**Default Configuration**

604800 seconds (30 days) is the default value for preferred-lifetime. 2592000 seconds (7 days) is the default value for valid-lifetime.

**Command Mode**

IPv6 DHCP Pool Configuration mode

**User Guidelines**

This command has no user guidelines.
Example
The following example defines a Multiple IPv6 prefix and client DUID within a pool for distributing to specific DHCPv6 Prefix delegation clients.

```console
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#prefix-delegation 2020::1/64
00:01:00:09:f8:79:4e:00:04:76:73:43:76
```

The following example defines a unique local address prefix with the MAC address 00:1D:BA:06:37:64 converted to EUI-64 format and a preferred lifetime of 5 days.

```console
console(config-dhcp6s-pool)#prefix-delegation fc00::/7
00:1D:BA:FF:FE:06:37:64 preferred-lifetime 43200
```

service dhcpv6
Use the `service dhcpv6` command in Global Configuration mode to enable local IPv6 DHCP server on the switch. Use the `no` form of the command to disable the DHCPv6 service.

**Syntax**

- `service dhcpv6`
- `no service dhcpv6`

**Default Configuration**

The service dhcpv6 is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

IPv6 DHCP relay and IPv6 DHCPv6 pool assignments require the DHCPv6 service to be enabled.

**Example**

The following example enables DHCPv6 globally.

```console
console#configure
console(config)#service dhcpv6
console(config)#no service dhcpv6
```
**show ipv6 dhcp**

Use the `show ipv6 dhcp` command to display the DHCPv6 server name and status.

**Syntax**

```
show ipv6 dhcp
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

The DUID value of the server will only appear in the output when a DHCPv6 lease is active.

**Example**

The following example displays the DHCPv6 server name and status.

```
console#show ipv6 dhcp
DHCPv6 is disabled
Server DUID:
```

**show ipv6 dhcp binding**

Use the `show ipv6 dhcp binding` command to display the configured DHCP pool.

**Syntax**

```
show ipv6 dhcp binding [ipv6-address]
```

- `ipv6-address` — Valid IPv6 address.

**Default Configuration**

This command has no default configuration.
**Command Mode**
Privileged Exec and User Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example displays the configured DHCP pool based on the entered IPv6 address.

```console
console#show ipv6 dhcp binding 2020:1::
```

**show ipv6 dhcp interface (User Exec)**
Use the `show ipv6 dhcp interface` command in User Exec mode to display DHCPv6 information for all relevant interfaces or for the specified interface. If an interface is specified, the optional statistics parameter is available to view statistics for the specified interface.

**Syntax**
```
show ipv6 dhcp interface [interface-id] [statistics]
```
- `interface-id`—A tunnel or VLAN interface identifier. See [Interface Naming Conventions](#) for interface representation.
- `statistics`—Enables statistics display if interface is specified.

**Default Configuration**
This command has no default configuration.

**Command Mode**
User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**
Statistics are shown depending on the interface mode (relay, server, or client).
Examples

The following examples display DHCPv6 information for VLAN 11 when configured in relay mode.

```
console> show ipv6 dhcp interface vlan 11
IPv6 Interface......................... vlan11
Mode..................................... Relay
Relay Address............................ 2020::1::1
Relay Interface Number.................... Relay
Relay Remote ID........................... Option Flags

console> show ipv6 dhcp interface vlan 11 statistics
DHCPv6 Interface vlan11 Statistics
-------------------------------------
DHCPv6 Solicit Packets Received......... 0
DHCPv6 Request Packets Received......... 0
DHCPv6 Confirm Packets Received......... 0
DHCPv6 Renew Packets Received........... 0
DHCPv6 Rebind Packets Received.......... 0
DHCPv6 Release Packets Received......... 0
DHCPv6 Decline Packets Received......... 0
DHCPv6 Inform Packets Received.......... 0
DHCPv6 Relay-forward Packets Received... 0
DHCPv6 Relay-reply Packets Received..... 0
DHCPv6 Malformed Packets Received...... 0
Received DHCPv6 Packets Discarded...... 0
Total DHCPv6 Packets Received........... 0
DHCPv6 Advertisement Packets Transmitted 0
DHCPv6 Reply Packets Transmitted........ 0
DHCPv6 Reconfig Packets Transmitted.... 0
DHCPv6 Relay-reply Packets Transmitted.. 0
DHCPv6 Relay-forward Packets Transmitted 0
Total DHCPv6 Packets Transmitted........ 0
```

**show ipv6 dhcp interface (Privileged Exec)**

Use the `show ipv6 dhcp interface` command to display configuration and status information about an IPv6 DHCP interface or all interfaces.

**Syntax**

```
show ipv6 dhcp interface [interface-id]{statistics}
```

- **interface-id**—Any valid IP interface. See `Interface Naming Conventions` for interface representation.
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines
This command shows the DHCP status. Information displayed depends on the mode.
The command output provides the following information for an interface configured in client mode. Not all fields will be shown for an inactive client.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Displays whether the specified interface is in Client, Relay, or Server mode.</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv6 Client on this interface. The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.</td>
</tr>
<tr>
<td>Server DUID</td>
<td>DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.</td>
</tr>
<tr>
<td>T1 Time</td>
<td>The T1 (in seconds) time as indicated by the DHCPv6 Server. T1 value indicates the time interval after which the address is requested for renewal.</td>
</tr>
<tr>
<td>T2 Time</td>
<td>The T2 (in seconds) time as indicated by the DHCPv6 Server. T2 value indicates the time interval after which the Client sends Rebind message to the Server in case there are no replies to the Renew messages.</td>
</tr>
<tr>
<td>Interface IAID</td>
<td>An identifier for an identity association chosen by this Client.</td>
</tr>
<tr>
<td>Leased Address</td>
<td>The IPv6 address leased by the DHCPv6 Server for this interface.</td>
</tr>
<tr>
<td>Preferred Lifetime</td>
<td>The preferred life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.</td>
</tr>
</tbody>
</table>
Example

The following example shows the output from this command when the device has leased an IPv6 address from the DHCPv6 server on interface Gi1/0/1.

**NOTE:** Note that the interface is in client mode.

```
console#show ipv6 dhcp interface vlan 2
IPv6 Interface................................. Vl2
Mode........................................... Client
State.......................................... ACTIVE
Server DUID.................................... 00:03:00:01:00:13:c4:db:6c:00
T1 Time........................................ 0 days 12 hrs 0 mins 0 secs
T2 Time........................................ 0 days 19 hrs 12 mins 0 secs
Interface IAID................................. 20
Leased Address................................. 2017::309D:161:4EF1:DBB1/128
Preferred Lifetime............................. 1 days 0 hrs 0 mins 0 secs
Valid Lifetime................................. 2 days 0 hrs 0 mins 0 secs
Renew Time..................................... 0 days 11 hrs 55 mins 28 secs
Expiry Time.................................... 1 days 23 hrs 55 mins 28 secs

console#show ipv6 dhcp interface vlan 10
IPv6 Interface................................. Vl10
Mode........................................... Relay
Relay Address.................................. 3030::3
Relay Interface Number......................... Relay
Relay Remote ID................................ Option Flags

console#show ipv6 dhcp interface vlan 10
IPv6 Interface................................. Vl10
Mode........................................... Server
Pool Name...................................... asd
Server Preference............................ 20

```

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Lifetime</td>
<td>The valid life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.</td>
</tr>
<tr>
<td>Renew Time</td>
<td>The time remaining (in seconds) to send a DHCPv6 Renew request to DHCPv6 Server for the leased address.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time (in seconds) when the DHCPv6 leased address expires.</td>
</tr>
</tbody>
</table>
Option Flags

console#show ipv6 dhcp interface vlan 10 statistics

DHCPv6 Server Interface Vl10 Statistics
DHCPv6 Solicit Packets Received............... 0
DHCPv6 Request Packets Received............... 0
DHCPv6 Confirm Packets Received............... 0
DHCPv6 Renew Packets Received............... 0
DHCPv6 Rebind Packets Received............... 0
DHCPv6 Release Packets Received............... 0
DHCPv6 Decline Packets Received............... 0
DHCPv6 Inform Packets Received............... 0
DHCPv6 Relay-forward Packets Received........ 0
DHCPv6 Relay-reply Packets Received........... 0
DHCPv6 Malformed Packets Received............. 0
Received DHCPv6 Packets Discarded............. 0
Total DHCPv6 Packets Received............... 0
DHCPv6 Advertisement Packets Transmitted..... 0
DHCPv6 Reply Packets Transmitted............. 0
DHCPv6 Reconfig Packets Transmitted......... 0
DHCPv6 Relay-reply Packets Transmitted....... 0
DHCPv6 Relay-forward Packets Transmitted.... 0
Total DHCPv6 Packets Transmitted............. 0

console#show ipv6 dhcp interface vlan 10 statistics

DHCPv6 Client Interface Vl10 Statistics

DHCPv6 Advertisement Packets Received........ 0
DHCPv6 Reply Packets Received............... 0
Received DHCPv6 Advertisement Packets Discarded 0
Received DHCPv6 Reply Packets Discarded....... 0
DHCPv6 Malformed Packets Received........... 0
Total DHCPv6 Packets Received............... 0
DHCPv6 Solicit Packets Transmitted........... 0
DHCPv6 Request Packets Transmitted........... 0
DHCPv6 Renew Packets Transmitted........... 0
DHCPv6 Rebind Packets Transmitted........... 0
DHCPv6 Release Packets Transmitted........... 0
Total DHCPv6 Packets Transmitted........... 0

show ipv6 dhcp pool

Use the show ipv6 dhcp pool command to display the configured DHCP pool.
**Syntax**

show ipv6 dhcp pool poolname

- poolname — Name of the pool. (Range: 1-32 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the configured DHCP pool.

```
console#show ipv6 dhcp pool test
DHCPv6 Pool: test
```

**show ipv6 dhcp statistics**

Use the `show ipv6 dhcp statistics` command in User Exec mode to display the global DHCPv6 server and relay statistics.

**Syntax**

show ipv6 dhcp statistics

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
This command has no user guidelines.

Example
The following example displays the DHCPv6 server name and status.

```
console> show ipv6 dhcp statistics
DHCPv6 Interface Global Statistics

        DHCPv6 Solicit Packets Received................. 0
        DHCPv6 Request Packets Received................ 0
        DHCPv6 Confirm Packets Received................ 0
        DHCPv6 Renew Packets Received................... 0
        DHCPv6 Rebind Packets Received.................. 0
        DHCPv6 Release Packets Received...............  0
        DHCPv6 Decline Packets Received...............  0
        DHCPv6 Inform Packets Received.................. 0
        DHCPv6 Relay-forward Packets Received.......... 0
        DHCPv6 Relay-reply Packets Received............ 0
        DHCPv6 Malformed Packets Received.............. 0
        Received DHCPv6 Packets Discarded.............. 0
        Total DHCPv6 Packets Received..................  0
        DHCPv6 Advertisement Packets Transmitted....... 0
        DHCPv6 Reply Packets Transmitted...............  0
        DHCPv6 Reconfig Packets Transmitted............ 0
        DHCPv6 Relay-reply Packets Transmitted......... 0
        DHCPv6 Relay-forward Packets Transmitted....... 0
        Total DHCPv6 Packets Transmitted...............  0
```
HiveAgent Commands

The commands in this section enable configuration of the Dell HiveAgent.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eula-consent</td>
<td>Use the <code>eula-consent</code> command to accept or decline the end-user license agreement (EULA) for the hive agent. If accepted, the latest version of the HiveAgent starts. If declined, all Hive Agent applications are stopped.</td>
</tr>
<tr>
<td>hiveagent url</td>
<td>Source interface VLAN ID</td>
</tr>
<tr>
<td>server show</td>
<td>Hive agent debug</td>
</tr>
<tr>
<td>debug show</td>
<td>Hive agent source interface</td>
</tr>
<tr>
<td>enable show</td>
<td>Hive agent status</td>
</tr>
<tr>
<td>proxy-ip-address</td>
<td>Show eula-consent hiveagent</td>
</tr>
</tbody>
</table>

**eula-consent**

Use the `eula-consent` command to accept or decline the end-user license agreement (EULA) for the hive agent. If accepted, the latest version of the HiveAgent starts. If declined, all Hive Agent applications are stopped.

**Syntax**

```
eula-consent {hiveagent} {accept | reject}
```

- **hiveagent**—Enter the keyword hiveagent to either accept or reject the EULA for the HiveAgent.
- **accept** — Accepts the EULA for the specified service.
- **reject** — Rejects the EULA for the specified service.

**Default Configuration**

The default is `eula-consent hiveagent accept`.

**Command Mode**

Global Configuration
**User Guidelines**

Messages are shown for both the accept and reject use cases with information directing the user to URLs for further information. If the user rejects or has not yet accepted the EULA, the configuration mode for the specified service is not usable. If there is existing configuration for that feature, the configuration is not removed, but the feature is disabled.

This command can be executed multiple times. It overwrites the previous information each time. The collected information is stored in the running-config. The administrator must write the configuration in order to persist it across reboots. If the administrator clears the config, this information must be reconfigured.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console(config)# eula-consent hiveagent accept
```

This switch includes a feature that enables it to work with HiveManager (an optional management suite), by sending the switch’s service tag number to HiveManager to authenticate your entitlement to use HiveManager. If you wish to disable this feature, you should run command “eula-consent hiveagent reject” immediately upon powering up the switch for the first time, or at any time thereafter.

```
console(config)# eula-consent hiveagent reject
```

I do not accept the terms of the license agreement. The HiveAgent feature has been deactivated and can no longer be used. To enable HiveAgent configurations, accept the terms of the license agreement by configuring this command 'eula-consent hiveagent accept'.

**hiveagent**

Use the **hiveagent** command to access the HiveAgent configuration mode. Use the **no** form of the command to remove the configured Dell HiveAgent information.

**Syntax**

`hiveagent`
no hiveagent

**Default Configuration**
By default, no HiveManager NG is configured by default.

**Command Mode**
Global Configuration

**User Guidelines**
This command enters HiveAgent Configuration mode. It allows the administrator to configure HiveAgent information. The configured information is stored in the running config. Use the write command to save the information into the startup-config.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
In this example, the HiveAgent EULA has been accepted.
```plaintext
corele(config)#hiveagent
corele(conf-hiveagent)#
```
In this example, the HiveAgent EULA has been rejected.
```plaintext
corele(config)#hiveagent
HiveAgent EULA has not been accepted. The HiveAgent cannot be configured until the HiveAgent EULA is accepted.
corele(config)#
```

**server**
Use the `server` command to configure a HiveAgent server (HiveManager NG) and enter HiveAgent server configuration mode. Use the `no` form of the command to remove a HiveAgent server.
**Syntax**

server server-name

no server server-name

server-name — The name of the server. The server name has a maximum length of 20 characters. Any printable character other than a question mark may be used in the server name. Enclose the server name in quotes if an embedded blank is desired in the server name.

**Default Configuration**

The default server HiveManagerNG is configured.

**Command Mode**

HiveAgent Configuration

**User Guidelines**

The server-name is used as a reference only and is not required to be used as part of a URL definition. The server name can consist of any alphanumeric character plus dashes or underscores.

Use the **exit** command to exit HiveAgent Server configuration mode.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

console(config)# hiveagent
console(conf-hiveagent)#server HiveManagerNG
console(conf-hiveagent-HiveManagerNG)#!

**debug**

Use the **debug** command to enable HiveAgent debug capability.

**Syntax**

debug
debug

no debug
**Default Configuration**
By default, HiveAgent debug is disabled.

**Command Mode**
HiveAgent Configuration mode

**User Guidelines**
This command enables HiveAgent debug.

**Command History**
Command introduced in version 6.5 firmware.

**Example**
```
console(config)#hiveagent
console(conf-hiveagent)#debug
```

**enable**
Use the `enable` command to enable a HiveAgent server. Use the `no` form of the command to disable a HiveAgent server.

**Syntax**
```
enable
no enable
```

**Default Configuration**
By default, the default server is enabled. It may be disabled using the `no enable` form of the command.

**Command Mode**
HiveAgent Server Configuration

**User Guidelines**
Only one HiveAgent server (HiveManager NG) can be enabled.
Command History
Introduced in version 6.3.0.1 firmware.

Example
console(config)# hiveagent
console(conf-hiveagent)#server HiveManagerNG
console(conf-hiveagent-HiveManagerNG)#enable

proxy-ip-address
Use the proxy-ip-address command to configure a proxy server to be used to contact the HiveManager NG. Use the no form of the command to remove the proxy server information.

Syntax
proxy-ip-address {ipv4-address | ipv6-address} port port-number username userid password [encryption-type] password
no proxy-ip-address

- ipv4-address — The IPv4 address of the proxy server in dotted decimal notation.
- ipv6-address — The IPv6 address of the proxy server in IPv6 notation.
- port-number — The TCP port number of the proxy server. The range is 1–65535. The default is 443.
- userid — The user name used to log into the proxy server.
- encryption-type— 0 indicates an unencrypted password; 7 indicates an encrypted password.
- password— An unencrypted or encrypted password. The maximum length is 64 characters for an unencrypted password. Encrypted passwords must be 128 characters in length.

Default Configuration
By default, no proxy is configured.
By default, passwords are entered as unencrypted and are always displayed and stored encrypted.
**Command Mode**
HiveAgent Server Configuration

**User Guidelines**
Passwords are always stored and displayed as encrypted, even if entered in unencrypted format.

**Example**
```
console(config)#support-assist
console(conf-support-assist)#server 10.0.0.1
console(conf-support-assist-10.0.0.1)#proxy-ip-address 10.0.0.2 port 1025
username admin password 0 password
```

**Command History**
Introduced in version 6.3.0.1 firmware.

**source-interface vlan-id**
Use the `source-interface vlan-id` command to assign a source interface which HiveAgent obtains the IP address used as the source IP address in packets addressed to the HiveManager NG.

**Syntax**
```
source-interface vlan-id <vlan-id>
no source-interface vlan-id
```
- `vlan-id`— A VLAN from which the IP address may be derived. Range 1–4093.

**Default Configuration**
By default, a source interface VLAN is not assigned.

**Command Mode**
HiveAgent Configuration mode
**User Guidelines**

The source VLAN must have an IP address assigned for it to be used by HiveAgent.

**Command History**

Command introduced in version 6.5 firmware.

**Example**

```console
console(config)#interface vlan 1
console(conf-vlan1)#ip address 172.16.32.11 /24
console(conf-vlan1)#exit

console(config)#hiveagent
console(conf-hiveagent)#source interface vlan-id 1
```

**url**

Use the `url` command to configure the URL to reach on HiveManager NG. Use the `no` form of the command to remove the URL information.

**Syntax**

```
url uniform-resource-locator
no url
```

- uniform-resource-locator — A text string for the URL using one of the following formats: hostip or hostname

**Default Configuration**

By default, the HiveManagerNG URL is cloud-<IP address>.aerohive.com.

**Command Mode**

HiveAgent Server Configuration

**User Guidelines**

The hostip for HiveManager NG may be specified as an IPv4 address, an IPv6 address or as a DNS hostname. If using the DNS hostname, the DNS resolver feature will need to be configured, enabled and operational.
**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
```
console(config)#hiveagent
console(conf-hiveagent)" server HiveManagerNG
console(conf-hiveagent-HiveManagerNG)#url cloud-rd.aerohive.com
```

**show hiveagent debug**
Use the `show hiveagent debug` command to view information on HiveAgent debug configuration. Status may also be obtained from the HiveManager NG web page.

**Syntax**
```
show hiveagent debug
```

**Default Configuration**
This command has no defaults.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all submodes

**User Guidelines**
There are no guidelines for this command.

**Command History**
Command introduced in version 6.5 firmware.

**Example**
```
console(config)# show hiveagent debug
```

**show hiveagent source-interface**
Use the `show hiveagent status` command to display the configured HiveAgent source interface.
Syntax
show hiveagent source-interface

Default Configuration
This command has no defaults.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
The source VLAN must have an IP address assigned for it to be used by HiveAgent.

Command History
Command introduced in version 6.5 firmware.

Example
console(config)# hiveagent
console(conf-hiveagent)#source interface vlan-id 1

show hiveagent status

Use the show hiveagent status command to display information on the HiveAgent configuration. The status can be obtained from the HiveManager NG web page.

Syntax
show hiveagent status

Default Configuration
This command has no defaults.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
There are no user guidelines for this command.

Command History
Introduced in version 6.3.0.1 firmware.

Example

```
console# show hiveagent status

HiveAgent: Enabled
EULA: Accepted
HiveManager Server Name: HiveManagerNG
HiveManager NG (enabled):
HiveAgent Version.............................. 1.0.1
HiveAgent Status............................... CONTACTING REDIRECTOR
HiveAgent AssociationUrl....................... -
HiveAgent AssociationMethod.................... REDIRECTOR
HiveAgent PollUrl.............................. -
HiveAgent RedirectorFQDN....................... cloud-rd.aerohive.com
HiveAgent RedirectorResponse................... CURL code [28], HTTP code [0], Curl string = [Timeout was reached]
```

show eula-consent hiveagent
Use the show eula-consent command to review the EULA details. Displaying the EULA details does not modify the current state of EULA acceptance for that feature.

Syntax

```
show eula-consent hiveagent
```

Default Configuration
The HiveAgent EULA is Accepted by default.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines
Acceptance of the HiveAgent EULA is enabled by default.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console#show eula-consent hiveagent

HiveAgent EULA has been: Accepted
This switch includes a feature that enables it to work with HiveManager (an optional management suite), by sending the switch’s service tag number to HiveManager to authenticate your entitlement to use HiveManager. If you wish to disable this feature, you should run command “eula-consent hiveagent reject” immediately upon powering up the switch for the first time, or at any time thereafter.
IP Addressing Commands

Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON/N4000 Series Switches

Interfaces on the Dell EMC Networking switches support a variety of capabilities to support management of the switch. In addition to performing switching and routing of network traffic, Dell EMC Networking switches act as a host for management of the switch. Commands in this category allow the network operator to configure the local host address, utilize the embedded DHCP client to obtain an address, resolve names to addresses using DNS servers, and detect address conflicts on the local subnet.

There are two management interface types on Dell EMC Networking switches. In-band interfaces allow management of the switch through the network switching/routing interfaces. Out-of-band management is always through the dedicated out-of-band interface. The serial port on the stack master provides a direct console interface supporting a CLI. In-band management interfaces can employ a variety of protection mechanisms including VLAN assignment and Management ACLs. The out-of-band port does not support such protection mechanisms and, therefore, it is recommended that the out-of-band interface only be connected to a physically segregated management network.

Commands in this Section

This section explains the following commands:

- clear host
- clear ip address-conflict-detect
- interface out-of-band
- ip address
- ip address (Out-of-Band)
- ip address-conflict-detect run
- ip address dhcp (Interface Configuration)
- ip default-gateway
- ip name-server source-interface
- ipv6 address
- ipv6 address dhcp
- ipv6 enable (Interface Configuration)
- ipv6 enable (OOB Configuration)
- ipv6 gateway (OOB Configuration)
- show hosts
- show ip address-conflict
clear host

Use the clear host command to delete entries from the host name-to-address cache.

**Syntax**

clear host {name | *}

- name — Host name to be deleted from the host name-to-address cache. (Range: 1-255 characters)
- * — Deletes all entries in the host name-to-address cache.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example deletes all entries from the host name-to-address cache.

```
console#clear host *
```

**clear ip address-conflict-detect**

Use the clear ip address-conflict-detect command to clear the address conflict detection status in the switch.
Syntax

clear ip address-conflict-detect [vrf vrf-name]

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, counters for the default (global) router instance is cleared.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned. Virtual Router Configuration mode is only available on the Dell EMC Networking N3000/N3100-ON/N4000 switches.

Example

console#clear ip address-conflict-detect

**interface out-of-band**

Use the `interface out-of-band` command to enter into OOB interface configuration mode.

Syntax

interface out-of-band

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration
User Guidelines

This command is not available on the N1100-ON/N1500/N2000 Series switches, nor on the N2128PX-ON switch.

Example

```
console(config)#interface out-of-band
console(config-if)#
```

ip address

Use the `ip address` command to configure an IP address on an in-band VLAN or loopback interface. Also use this command to configure one or more secondary IP addresses on the interface.

Syntax

```
ip address ip-address {{subnet-mask | prefix-length} [secondary] | dhcp | none}
```

```
no ip address ip-address {subnet-mask | prefix-length} [secondary]
```

- `ip-address` — IP address of the interface.
- `dhcp` — Obtain the address from a DHCP server.
- `none` — Clear the address assignment method.
- `subnet-mask` — Subnet mask of the interface
- `prefix-length` — Length of the prefix. Must be preceded by a forward slash (/). (Range: 1-30 bits)
- `secondary` — Indicates the IP address is a secondary address.

Default Configuration

The N1100/N1500/N2000/N2100-ON default IPv4 address assignment method is DHCP on VLAN 1.

The N3000/N3100/N4000 default IPv4 address assignment method on VLAN 1 is none, and the default address assignment on the out-of-band port is DHCP. See the `ip address (Out-of-band)` command for more information.

Use the `no interface vlan` command to remove an IP routing interface, clear any bound IP address and set the address assignment method to the default.
Command Mode
Interface Configuration (VLAN, Loopback) mode

User Guidelines
This command also implicitly enables the VLAN or loopback interface for routing (i.e. as if the user had issued the ‘routing’ interface command). By default, configuring an IP address on a VLAN enables in-band management for interfaces configured with that VLAN. Setting up an IP address on VLAN 1 enables switch management on all in-band interfaces except for those where VLAN 1 is specifically excluded.

The `ip address none` command clears the currently assigned IPv4 address and sets the IP address configuration method to `none`. The `no ip address` command clears the currently assigned IPv4 address and sets the IP address configuration method to the default (whatever the default is).

Use the `show ip interface {management|vlan <vlanid>}` command to display the configured IP addresses.

A physical or loopback interface must be made a member of the VLAN in order for the address configuration to be bound to an interface.

A VLAN interface configured for DHCP address assignment will send the following text string in DHCP Option 60 of the DHCPDISCOVER message to assist the DHCP server in identification of the switch: "DellEMC;<switch model>;<firmware version>;<serial number>". The left and right angle brackets and quotation marks are not sent. An example option 60 string might be: DellEMC;N2128PX-ON;6.5.2.0;TW06G93K282986CR0040

IP addresses assigned to Ethernet interfaces support up to 31 bit subnet masks. IP addresses assigned to loopback ports support a full 32 bit subnet mask.

Example
The following example defines the IP address and subnet mask for VLAN 15 and enables the VLAN for routing.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip address 192.168.10.10 255.255.255.0
```
ip address (Out-of-Band)

Use the ip address command in Interface Configuration mode to set an IP address for the out-of-band interface. Use the no form of this command to return the ip address configuration to its default value.

Syntax

ip address {ip-address {mask | prefix-length} | dhcp | none}
no ip address

- ip-address—Specifies a valid IPv4 address in dotted-quad notation.
- mask—Specifies a valid subnet (network) mask IPv4 address in dotted quad notation.
- prefix-length—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1-30 bits)
- dhcp—Obtain the out-of-band interface address via DHCPv4.

Default Configuration

The out-of-band interface (service port) obtains an IP address via DHCP by default.

Command Mode

Interface (Out-of-Band) Configuration mode

User Guidelines

When setting the netmask/prefix length on an IPv4 address, a space is required between the address and the mask or prefix length. Setting an IP address on the out-of-band port enables switch management over the out-of-band port.

The ip address none command clears the currently assigned IPv4 address and sets the IP address configuration method to none. The no ip address command clears the currently assigned IPv4 address and sets the IP address configuration method to the default (dhcp).
A out-of-band interface configured for DHCP address assignment will send the following text string in DHCP Option 60 of the DHCPDISCOVER message to assist the DHCP server in identification of the switch: "DellEMC;<switch model>;<firmware version>;<serial number>". The left and right angle brackets and quotation marks are not sent. An example option 60 string might be: DellEMC;N2128PX-ON;6.5.2.0;TW06G93K282986CR0040

In order to ensure the security of the switches from intruders, it is strongly recommended that the out-of-band interface be isolated on a physically separate network from the in-band ports. This command is only valid for switches equipped with an out-of-band interface.

**Example**

The following examples configure the out-of-band interface with an IP address 131.108.1.27 and subnet mask 255.255.255.0 and the same IP address with prefix length of 24 bits.

```
console(config)#interface out-of-band
console(config-if)#ip address 131.108.1.27 255.255.255.0
console(config-if)#ip address 131.108.1.27 /24
```

**ip address-conflict-detect run**

Use the `ip address-conflict-detect run` command in Global Configuration mode to trigger the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

**Syntax**

```
ip address–conflict–detect run
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode, Virtual Router Configuration mode.
**User Guidelines**

When in virtual router configuration mode, this command operates within the context of the virtual router instance. When in global config mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the Dell EMC Networking N3000/N3100-ON/N4000 switches.

**Example**

```
console#configure
code(config)#ip address-conflict-detect run
```

**ip address dhcp (Interface Configuration)**

Use the `ip address dhcp` command in Interface (VLAN) Configuration mode to enable the DHCPv4 client on an interface.

**Syntax**

- `ip address dhcp`
- `no ip address dhcp`

**Default Configuration**

DHCPv4 is disabled by default on routing interfaces.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

This command only applies to VLAN routing interfaces. When DHCP is enabled on a routing interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

- The command `no ip address` removes the interface’s primary address (Manual/DHCP) including the secondary addresses, if configured, and sets the Interface method to `None`.
- The command `no ip address dhcp` removes the interface’s primary address only if configured through DHCP and sets the interface method to `None`. It does not remove a manually configured address.
In addition to leasing an IP address and subnet mask, the DHCP client may learn the following parameters from a DHCP server:

- The IPv4 address of a default gateway. If the device learns different default gateways on different interfaces, the system uses the first default gateway learned. The system installs a default route in the routing table, with the default gateway’s address as the next hop address. This default route has a preference of 254.
- The IPv4 address of a DNS server. The DNS client stores each DNS server address in its server list.
- A domain name. The DNS client stores each domain name in its domain name list.

A VLAN routing interface configured for DHCP address assignment will send the following text string in DHCP Option 60 of the DHCPDISCOVER message to assist the DHCP server in identification of the switch: "DellEMC;<switch model>;<firmware version>;<serial number>". The left and right angle brackets and quotation marks are not sent. An example option 60 string might be: DellEMC;N2128PX-ON;6.5.2.0;TW06G93K282986CR0040

**Examples**

To enable DHCPv4 on vlan 2:

```
console#config
console(config)#interface vlan 2
console(config-if-vlan2)#ip address dhcp
```

**ip default-gateway**

Use the `ip default-gateway` command to configure a default gateway (router).

**Syntax**

```
ip default-gateway ip-address
no ip default-gateway ip-address
```

- `ip-address`—Valid IPv4 address of an attached router.

**Default Configuration**

No default gateway is defined.


**Command Mode**

Global Configuration mode, Virtual Router Configuration mode

**User Guidelines**

When the system does not have a more specific route to a packet’s destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server, which has a route preference of 254. It is less preferred than a static route configured via the `ip route` command, which has a route preference of 1. Use the `show ip route` command to display the active default gateway.

Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value. When in Virtual Router Configuration mode, this command operates within the context of the virtual router instance. When in Global Configuration mode, the command operates on the global router instance.

Virtual Router Configuration mode is only available on the Dell EMC Networking N3000/N3100-ON/N4000 switches.

Setting a default gateway on the in-band network may make indirectly connected hosts on the out-of-band network unreachable. Dell EMC N1100-ON switches support configuration of a single default gateway. If a subsequent gateway is configured, the prior configuration is overwritten. Dell EMC N1100-ON switches do not support routing.

**Example**

The following example sets the default-gateway to 10.1.1.1.

```console
console(config)#ip default-gateway 10.1.1.1.
```

**ip domain-lookup**

Use the `ip domain-lookup` command in Global Configuration mode to enable IP Domain Naming System (DNS)-based host name-to-address translation. To disable the DNS, use the `no` form of this command.
Syntax
ip domain-lookup
no ip domain-lookup

Default Configuration
DNS name resolution is enabled by default.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example enables the IP Domain Naming System (DNS)-based host name-to-address translation.

console(config)#ip domain-lookup

ip domain-name

Use the ip domain-name command in Global Configuration mode to define a default domain name used to complete unqualified host names. To delete the default domain name, use the no form of this command.

Syntax
ip domain-name name
no ip domain-name

- name — Default domain name used to complete an unqualified host name. Do not include the initial period that separates the unqualified host name from the domain name (Range: 1-255 characters).

Default Configuration
This command has no default configuration.
Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example defines a default domain name of dell.com.

```
console(config)#ip domain-name dell.com
```

ip host
Use the `ip host` command in Global Configuration mode to define static host name-to-address mapping in the host cache. To delete the name-to-address mapping, use the `no` form of this command.

Syntax

```
ip host name address
no ip host name
```

- name — Host name.
- address — IP address of the host.

Default Configuration
No host is defined.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example defines a static host name-to-address mapping in the host cache.
ip name-server

Use the `ip name-server` command in Global Configuration mode to define available IPv4 or IPv6 name servers. To delete a name server, use the `no` form of this command.

**Syntax**

```
ip name-server server-address1 [server-address2 ... server-address8]
no ip name-server [server-address1 ... server-address8]
```

- **server-address** — Valid IPv4 or IPv6 addresses of the name server. (Range: 1–255 characters)

**Default Configuration**

No name server IP addresses are specified.

**Command Mode**

Global Configuration mode

**User Guidelines**

Server preference is determined by entry order.

Up to eight servers can be defined in one command or by using multiple commands. Use the `show hosts` command to display the configured name servers.

**Example**

The following example sets the available name server.

```
console(config)#ip name-server 176.16.1.18
```

ip name-server source-interface

Use the `ip name-server source-interface` command to select the interface from which to use the IP address in the source IP address field of transmitted DNS packets. To revert to the default IP address, use the `no` form of this command.
Syntax

ip name-server source-interface {loopback loopback-id | tunnel tunnel-id | vlan vlan-id }

no ip name-server source-interface
  • loopback-id—A loopback interface identifier.
  • tunnel-id—A tunnel identifier.
  • vlan-id—A VLAN identifier.

Default Configuration

By default, the switch uses the assigned switch IP address as the source IP address for DNS packets. This address is either the IP address assigned to the VLAN from which the DNS packet originates or the out-of-band interface IP address.

Command Mode

Global Configuration mode

User Guidelines

The source interface must have an assigned IP address (assigned either manually or via another method such as DHCP).

The use of a source interface allows firewalls devices to identify DNS packets as coming from a specific switch. If the source interface is not specified, the primary address of the outbound interface is used as the source interface. If the specified interface is down, the DNS client falls back to it’s original (unconfigured) behavior.

This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

Command History

Introduced in version 6.3.0.1 firmware.
**Example**

The following example configures a source interface for a VLAN interface that obtains its address via DHCP:

```plaintext
console#configure
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#ip name-server source-interface vlan 1
```

This example configures a source interface for a loopback interface. Using a loopback address is the recommended method for assigning a source interface.

```plaintext
console#configure
console(config)#interface loopback 0
console(config-if-vlan1)#ip address 129.168.0.13 /32
console(config-if-vlan1)#exit
console(config)#ip name-server source-interface vlan 1
```

**ipv6 address (Interface Configuration)**

Use the `ipv6 address` command to set the IPv6 address of an interface. Use the `no` form of this command to reset the IPv6 address to the default.

**Syntax**

```plaintext
ipv6 address {prefix/prefix-length [eui64] | autoconfig | dhcp}
no ipv6 address
```

- **prefix**—The IPv6 address to be configured.
- **prefix-length**—Designates how many of the high-order contiguous bits of the address make up the prefix.
- **eui64**—The optional EUI-64 field designates that IPv6 processing on the interfaces is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, the value of prefix_length must be 64 bits.
- **autoconfig**—Use this keyword to enable IPv6 address auto configuration mode.
- **dhcp**—Use this keyword to obtain an IPv6 address via DHCP.
**Default Configuration**

There is no IPv6 address configured by default.

**Command Mode**

Interface Configuration mode (VLAN, tunnel, loopback)

**User Guidelines**

When setting the prefix length on an IPv6 address, no space can be present between the address and the mask.

Multiple globally reachable addresses may be assigned to an interface. Creation of a link local address is automatically performed by this command.

IPv6 addresses may be expressed in up to eight blocks. For simplification, the leading zeros of each 16 bit block may be omitted. One sequence of 16 bit blocks—containing only zeros—may be replaced by a double colon”::”, but not more than one at a time.

- Dropping zeros: 3ffe:ffff:100::f101::0:0:1 becomes 3ffe:ffff:100:f101:1
- Local host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
- Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in IPv6 addresses are not case sensitive.

The optional eui64 parameter indicates that the IPv6 address is configured to use the EUI-64 interface ID in the low order 64 bits of the address. If this parameter is specified, the prefix-length must be 64.

**Example**

Configure IPv6 routing on vlan 10 and obtain an address via DHCP. Assumes vlan 10 already exists.

```console
console(config)#ip routing
console(config)#interface vlan 10
console(config-if-vlan10)#ipv6 enable
console(config-if-vlan10)#ipv6 address dhcp
Configure a default gateway on vlan 10
console(config)#no ipv6 address autoconfig
console(config)#no ipv6 address 2003::6/64
console(config)#no ipv6 address 2001::/64 eui64
console(config)#no ipv6 address
```
**ipv6 address (OOB Port)**

Use the `ipv6 address` command in Interface (out-of-band) Configuration mode to set the IPv6 prefix on the out-of-band port. If a prefix is specified, the address will be configured using the prefix and length. A link local address in EUI-64 format may also be assigned.

The `autoconfig` parameter specifies that a link local address in the EUI-64 format is assigned to the interface.

The `DHCP` parameter indicates that the port should obtain its address via DHCP.

Use the `no` form of the command to remove a specific address or to return the address assignment to its default value. Using the `no` form of the command with no parameters removes all IPv6 prefixes from the interface.

**Syntax**

```
ipv6 address {prefix/prefix-length [eui64] | autoconfig | dhcp}
```

```
no ipv6 address {prefix/prefix-length [eui64] | autoconfig | dhcp}
```

- `prefix/prefix-length`—An IPv6 prefix in global format address format.
- `eui64`—Formulate the prefix in EUI-64 format.
- `autoconfig`—Perform IPv6 auto-configuration.
- `dhcp`—Obtain the prefix via DHCP.

**Default Configuration**

No address is assigned to the out-of-band interface by default.

**Command Mode**

Interface (out-of-band) Configuration mode

**User Guidelines**

When DHCPv6 is enabled on the Out-of-Band interface, the system automatically deletes all manually configured IPv6 addresses on the interface.

DHCPv6 can be enabled on the Out-of-Band interface only when IPv6 auto configuration or DHCPv6 is not enabled on any of the in-band management interfaces.
IPv6 auto configuration mode can be enabled in the Out-of-Band interface only when IPv6 auto configuration or DHCPv6 is not enabled on any of the in-band management interfaces.

The optional eui64 parameter indicates that the IPv6 address is configured to use the EUI-64 interface ID in the low order 64 bits of the address. In this parameter is specified, the prefix-length must be 64. This command is only valid for switches equipped with an out-of-band interface.

**ipv6 address dhcp**

Use the `ipv6 address dhcp` command in Interface (VLAN) Configuration mode to enable the DHCPv6 client on an IPv6 interface.

**Syntax**

```
ipv6 address dhcp
no ipv6 address dhcp
```

**Default Configuration**

DHCPv6 is disabled by default on routing interfaces.

**Command Mode**

Interface (VLAN) Configuration mode

**User Guidelines**

This command only applies to VLAN routing interfaces. When DHCPv6 is enabled on a VLAN routing interface, the system automatically deletes all manually configured IPv6 addresses on the interface.

Use the `no ipv6 address dhcp` command to release a leased address and to disable DHCPv6 on an interface. The command `no ipv6 address` does not disable the DHCPv6 client on the interface.

This command will fail if DHCPv6 server has been configured on the interface.

**Examples**

In the following example, DHCPv6 is enabled on interface vlan2.
ipv6 enable (Interface Configuration)

Use the `ipv6 enable` command in Interface Configuration mode to enable IPv6 on a routing interface. Use the `no` form of this command to reset the IPv6 configuration to the defaults.

**Syntax**

ipv6 enable  
no ipv6 enable

**Default Configuration**

IPv6 is not enabled by default.

**Command Mode**

Interface Configuration mode (VLAN, tunnel, loopback)

**User Guidelines**

There are no user guidelines for this command.

**Example**

```
console(config)#no ipv6 enable
```

ipv6 enable (OOB Configuration)

Use the `ipv6 enable` command in Interface (out-of-band) Configuration mode to enable IPv6 operation on the out-of-band interface. Prefixes configured by the ipv6 address command are not configured until the interface is enabled.

**Syntax**

ipv6 enable  
no ipv6 enable
**Default Configuration**
By default, IPv6 is not enabled on the out-of-band port.

**Command Mode**
Interface (out-of-band) Configuration mode

**User Guidelines**
This command is not necessary if an IPv6 address has been assigned to the interface. This command is only valid for switches equipped with an out-of-band interface.

**ipv6 gateway (OOB Configuration)**
Use the `ipv6 gateway` command in Interface (out-of-band) Configuration mode to configure the address of the IPv6 gateway. The gateway is used as a default route for packets addressed to network devices not present on the local subnet. Use the `no` form of the command to remove the gateway configuration.

**Syntax**
ipv6 gateway ipv6-address
no ipv6 gateway
  • ipv6-address—An IPv6 address (not a prefix).

**Default Configuration**
By default, no IPv6 gateway is configured.

**Command Mode**
Interface (out-of-band) Configuration mode

**User Guidelines**
This command is only valid for switches equipped with an out-of-band interface.
show hosts

Use the **show hosts** command in User Exec mode to display the default domain name, a list of name server hosts, and the static and cached list of host names and addresses.

**Syntax**

```bash
show hosts [hostname].
```

- **hostname**—(Range: 1–255 characters). The command allows spaces in the host name when specified in double quotes. For example, `console(config)#show hosts "host name"`

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays information about IP hosts.

```bash
console>show hosts
Host name: dellswitch
Default domain: dell.com
Name/address lookup is enabled
DNS source interface: loopback 1
Name servers (Preference order): 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting.dell.com</td>
<td>176.16.8.8</td>
</tr>
</tbody>
</table>

Cache:

<table>
<thead>
<tr>
<th>Host</th>
<th>Total</th>
<th>Elapsed</th>
<th>Type</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.stanford.edu">www.stanford.edu</a></td>
<td>72</td>
<td>3</td>
<td>IP</td>
<td>171.64.14.203</td>
</tr>
</tbody>
</table>
show ip address-conflict

Use the `show ip address-conflict` command in User Exec or Privileged Exec mode to display the status information corresponding to the last detected address conflict.

**Syntax**

```
show ip address-conflict [vrf vrf-name]
```
- `vrf-name`—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100-ON/N4000 series switches.

The command provides the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Conflict</td>
<td>Whether the switch has detected an address conflict on any IP address. Set to Conflict Detected if detected, No Conflict Detected otherwise.</td>
</tr>
<tr>
<td>Detection Status</td>
<td></td>
</tr>
<tr>
<td>Last Conflicting IP</td>
<td>The IP address that was last detected as conflicting on any interface.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Last Conflicting MAC</td>
<td>The MAC Address of the conflicting host that was last detected on any interface.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
</tbody>
</table>
Example

console#show ip address-conflict

Address Conflict Detection Status...Conflict Detected
Last Conflicting IP Address........10.131.12.56
Last Conflicting MAC Address.......00:01:02:04:5A:BC
Time Since Conflict Detected........5 days 2 hrs 6 mins 46 secs

console#show ip address-conflict

Address Conflict Detection Status........... No Conflict Detected

**show ip helper-address**

Use the `show ip helper-address` command to display IP helper addresses configuration.

**Syntax**

`show ip helper-address [vrf vrf-name][intf-address]`

- vrf-name—The name of the VRF instance on which the command operates. If no VRF parameter is given, information for the default (global) router instance is shown.
- intf-address — IP address of a routing interface in dotted quad notation.
  (Range: Any valid IP address)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes
User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.

The VRF parameter is only available on the N3000/N3100-ON/N4000 series switches. This command is not available on the N1100-ON Series switches.

Example

```
console#show ip helper-address

IP helper is enabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>UDP Port</th>
<th>Discard</th>
<th>Hit Count</th>
<th>Server Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 25</td>
<td>domain</td>
<td>No</td>
<td>0</td>
<td>192.168.40.2</td>
</tr>
<tr>
<td>vlan 25</td>
<td>dhcp</td>
<td>No</td>
<td>0</td>
<td>192.168.40.2</td>
</tr>
<tr>
<td>vlan 30</td>
<td>dhcp</td>
<td>Yes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>vlan 30</td>
<td>162</td>
<td>No</td>
<td>0</td>
<td>192.168.23.1</td>
</tr>
<tr>
<td>Any</td>
<td>dhcp</td>
<td>No</td>
<td>0</td>
<td>192.168.40.1</td>
</tr>
</tbody>
</table>
```

show ipv6 dhcp interface out-of-band statistics

Use the `show ipv6 dhcp interface out-of-band statistics` command to display IPv6 DHCP statistics for the out-of-band interface.

Syntax

```
show ipv6 dhcp interface out-of-band statistics
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

This command is only supported on platforms equipped with an out-of-band port.
Example

console#show ipv6 dhcp interface out-of-band statistics

DHCPv6 Client Statistics
-------------------------
DHCPv6 Advertisement Packets Received........ 0
DHCPv6 Reply Packets Received.................. 0
Received DHCPv6 Advertisement Packets Discard.. 0
Received DHCPv6 Reply Packets Discarded........ 0
DHCPv6 Malformed Packets Received.............. 0
Total DHCPv6 Packets Received.................. 0
DHCPv6 Solicit Packets Transmitted.............. 8
DHCPv6 Request Packets Transmitted............. 0
DHCPv6 Renew Packets Transmitted............... 0
DHCPv6 Rebind Packets Transmitted............... 0
DHCPv6 Release Packets Transmitted............. 0
Total DHCPv6 Packets Transmitted............... 8

show ipv6 interface out-of-band

Use the show ipv6 interface out-of-band command to show the IPv6 out-of-band port configuration.

Syntax

show ipv6 interface out-of-band

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

This command is only available on switches equipped with an out-of-band interface.

Example

console(config-if)#show ipv6 interface out-of-band
IPv6 Administrative Mode........Enabled
IPv6 Prefix is.................FE80::21E:C9FF:FEAA:AD79/64
::/128
IPv6 Default Router............FE80::A912:FEC2:A145:FEAD
Configured IPv6 Protocol........None
IPv6 AutoConfiguration mode.........Enabled
Burned In MAC Address..........001E.C9AA.AD79
Line Commands

This section explains the following commands:

<table>
<thead>
<tr>
<th>accounting</th>
<th>line</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorization</td>
<td>login authentication</td>
</tr>
<tr>
<td>enable authentication</td>
<td>login-banner</td>
</tr>
<tr>
<td>exec-banner</td>
<td>motd-banner</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>password (Line Configuration)</td>
</tr>
<tr>
<td>history</td>
<td>show line</td>
</tr>
<tr>
<td>history size</td>
<td>speed</td>
</tr>
<tr>
<td></td>
<td>terminal length</td>
</tr>
</tbody>
</table>

Authentication commands related to line configuration mode are in DHCP Client Commands.

accounting

Use the **accounting** command in Line Configuration mode to apply an accounting method to a line config.

Use the **no** form of the command to return the accounting for the line mode to the default.

**Syntax**

```
accounting {exec|commands} [default|list-name]

no accounting
```

- **exec**—Provides accounting for a user Exec terminal session.
- **commands**—Provides accounting for all user-executed commands.
- **default**—The default list of methods for accounting services.
- **list-name**—Character string of not more than 15 characters used to name the list of accounting methods. The list name can consist of any printable character other than a question mark. Use quotes around the list name if embedded blanks are contained in the list name.
**Default Configuration**

Accounting is not enabled by default.

**Command Mode**

Line Configuration

**User Guidelines**

When enabling accounting for exec mode for the current line-configuration type, users logged in with that mode will be logged out.

**Examples**

Use the following command to enable exec type accounting for telnet.

```
console(config)#line telnet
console(config-telnet)# accounting exec default
```

**authorization**

Use the `authorization` command to apply a command authorization method to a line config. Use the `no` form of the command to return the authorization for the line mode to the default.

**Syntax**

```
authorization {commands|exec} [default|list-name]
no authorization {commands|exec}
```

- **commands**—Perform authorization for each command entered by the user.
- **exec**—Perform Exec authorization for the user (authorization required to enter privileged Exec mode).
- **default**—The default list of methods for command authorization (cmdAuthList).
- **list-name**—Character string used to name the list of authorization methods. The list name can consist of any printable character other than a question mark. Use quotes around the list name if embedded blanks are contained in the list name.
Default Configuration
Authorization is not enabled on any line method by default.

Command Mode
Line console, line telnet, line SSH

User Guidelines
When command authorization is configured for a line-mode, the switch sends information about the entered command to the method specified in the command list. The authorization method validates the received command and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. If contact with the authorization method fails, then the next method in the list is attempted.

Examples
Use the following command to enable TACACS command authorization for telnet.

```
console(config)#line telnet
console(config-telnet)# authorization commands mycmdAuthList
```

enable authentication

Use the `enable authentication` command in Line Configuration mode to specify the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default specified by the `enable authentication` command, use the `no` form of this command.

Syntax

```
enable authentication {default | list-name}
```

```
no enable authentication
```

- default — Uses the default list created with the `aaa authentication enable` command.
- list-name — Uses the indicated list created with the `aaa authentication enable` command. (Range: 1-12 characters)
Default Configuration
Uses the default set with the command `aaa authentication enable`.

Command Mode
Line Configuration mode

User Guidelines
Use of the no form of the command does not disable authentication. Instead, it sets the authentication list to the default list (same as enable authentication default).

Example
The following example specifies the default authentication method when accessing a higher privilege level console.

```console
console(config)# line console
console(config-line)# enable authentication default
```

exec-banner
Use the `exec-banner` command to enable exec banner on the console, telnet or SSH connection. To disable, use the `no` form of the command.

Syntax
exec-banner
no exec-banner

- MESSAGE — Quoted text

Default Configuration
This command has no default configuration.

Command Mode
Line Configuration
**User Guidelines**

The exec banner can consist of multiple lines. Enter a quote to complete the message and return to configuration mode.

**Example**

```console
console(config-telnet)# no exec-banner
```

**exec-timeout**

Use the `exec-timeout` command in Line Configuration mode to set the interval that the system waits for user input before timeout. To restore the default setting, use the `no` form of this command.

**Syntax**

```
exec-timeout minutes [seconds]
no exec-timeout
```

- minutes — Integer that specifies the number of minutes. (Range: 0–65535)
- seconds — Additional time intervals in seconds. (Range: 0–59)

**Default Configuration**

The default configuration is 10 minutes.

**Command Mode**

Line (telnet, console, ssh) Configuration mode

**User Guidelines**

To specify no timeout, enter the `exec-timeout 0` command.

**Example**

The following example configures the interval that the system waits until user input is detected to 20 minutes. After expiry, the session exits Privileged Exec mode.

```console
console(config)#line console
console(config-line)#exec-timeout 20
```
**history**

Use the `history` command in Line Configuration mode to enable the command history function. To disable the command history function, use the `no` form of this command.

**Syntax**

```
history
no history
```

**Default Configuration**

The default value for this command is enabled.

**Command Mode**

Line Interface mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example disables the command history function for the current terminal session.

```
console(config-line)# no history
```

**history size**

Use the `history size` command in Line Configuration mode to change the command history buffer size for a particular line. To reset the command history buffer size to the default setting, use the `no` form of this command.

**Syntax**

```
history size number-of-commands
no history size
```

- `number-of-commands`—Specifies the number of commands the system may record in its command history buffer. (Range: 0-216)
**Default Configuration**
The default command history buffer size is 10.

**Command Mode**
Line Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures the command history buffer size to 20 commands for the current terminal session.

```console
console(config-line)#history size 20
```

**line**
Use the `line` command in Global Configuration mode to identify a specific line for configuration and enter the line configuration command mode.

**Syntax**
```
line {console | telnet | ssh}
```
- `console` — Console terminal line.
- `telnet` — Virtual terminal for remote console access (Telnet).
- `ssh` — Virtual terminal for secured remote console access (SSH).

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode
User Guidelines

The default authentication list for telnet and SSH is enableNetList. The enableNetList uses a single method: enable. This implies that users accessing the switch via telnet or SSH must have an enable password defined in order to access privileged mode. Alternatively, the administrator can set the telnet and ssh lists to enableList, which has the enable and none methods defined.

When using line ssh authentication with a RADIUS server as the primary authentication method, be aware that the default 802.1x timeout is 45 seconds. This is the same timeout value as SSH. Thus a secondary authentication method is unlikely to be invoked due to SSH timing out and dropping the connection attempt.

Examples

The following example sets the telnet authentication list to enableList:

```
console(config)#line telnet
console(config-telnet)#enable authentication enableList
```

The following example enters Line Configuration mode to configure Telnet:

```
console(config)#line telnet
console(config-line)#
```

login authentication

Use the login authentication command in Line Configuration mode to specify the login authentication method list for a line (console, telnet, or SSH). To return to the default specified by the authentication login command, use the no form of this command.

Syntax

```
login authentication {default | list-name}
no login authentication
```

- default — Uses the default list created with the aaa authentication login command.
- list-name — Uses the indicated list created with the aaa authentication login command.
**Default Configuration**
Uses the default set with the command `aaa authentication login`.

**Command Mode**
Line Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example specifies the default authentication method for a console.

```
console(config)# line console
console(config-line)# login authentication default
```

**login-banner**
Use the `login-banner` command to enable login banner on the console, telnet or SSH connection. To disable, use the `no` form of the command.

**Syntax**

```
login-banner
no login-banner
```

- MESSAGE — Quoted text

**Default Configuration**
This command has no default configuration.

**Command Mode**
Line Configuration

**User Guidelines**
This command has no user guidelines.
Example

```
console(config-telnet)# no login-banner
```

**motd-banner**

Use the *motd-banner* command to enable motd on the console, telnet or SSH connection. To disable, use the *no* form of the command.

**Syntax**

```
motd-banner
no motd-banner
```

-  **MESSAGE** — Quoted text

**Default Configuration**

This command has no default configuration.

**Command Mode**

Line Configuration

**User Guidelines**

This command has no user guidelines.

**Example**

```
console(config-telnet)# motd-banner
```

**password (Line Configuration)**

Use the *password* command in Line Configuration mode to specify a password on a line. To remove the password, use the *no* form of this command.

⚠️ **NOTE:** For commands that configure password properties, see Password Management Commands.

**Syntax**

```
password password [encrypted]
no password
```
Switch Management Commands

- **password** — Password for this level. (Range: 8-64 characters) The special characters allowed in the password include ! # $ % & ‘ ( ) * + , - . / ; < = > @ [ \ ] ^ _ ` { | } ~. User names can contain blanks if the name is surrounded by double quotes.

- **encrypted** — Encrypted password to be entered, copied from another switch configuration.

**Default Configuration**

No password is specified.

**Command Mode**

Line Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example specifies a password “mcmxxyyy” on a line.

```
console(config-line)# password mcmxxyyy
```

**show line**

Use the `show line` command to display line parameters.

**Syntax**

```
show line [console | telnet | ssh]
```

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

**Default Configuration**

This command has no default configuration.
**Command Mode**
User Exec and Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
```
console(config-telnet)#show line
```

Console configuration:
Serial Port Login Timeout (mins) (secs)........ 10 minutes 0 seconds
Baud Rate (bps)................................ 9600
Character Size (bits).......................... 8
Flow Control................................... Disable
Stop Bits...................................... 1
Parity......................................... none
History:....................................... 10

Telnet configuration:
Remote Connection Login Timeout(mins)(secs)... 10 minutes 0 seconds
History:....................................... 10

SSH configuration:
Remote Connection Login Timeout(mins)(secs)... 10 minutes 0 seconds
History:....................................... 10

**speed**
Use the `speed` command in Line Configuration mode to set the line BAUD rate. Use the `no` form of the command to restore the default settings.

**Syntax**
```
speed {bps}
no speed
```
- bps — BAUD rate in bits per second (bps). The options are 2400, 9600, 19200, 38400, 57600, and 115200.
Default Configuration
This default speed is 9600 for all platforms other than the N1100-ON/N2100/N3100 Series switches. The N1100-ON/N2100/N3100 Series switches default to 115200 BAUD.

Command Mode
Line Interface (console) mode

User Guidelines
This configuration applies only to the current session.

Example
The following example configures the console BAUD rate to 9600.

```
console(config-line)#speed 9600
```

terminal length
Use the terminal length command to set the terminal length. Use the no form of the command to reset the terminal length to the default.

Syntax
```
terminal length value
no terminal length
```

- value — The length in number of lines. Range: 0–512

Default Configuration
This default value is 24.

Command Mode
Privileged Exec mode
**User Guidelines**

Setting the terminal length to 0 disables paging altogether. It is recommended that the terminal length either be set to 0 or a value larger than 4 as terminal lengths in the range of 1 to 4 may give odd output due to prompting. The terminal length command is specific to the current session. Logging out, rebooting or otherwise ending the current session will require that the command be reentered. Likewise, because the terminal length setting is specific to a session, it is never saved in the config.

**Example**

c console#terminal length 50
PHY Diagnostics Commands

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show copper-ports tdr</td>
<td>Display the stored information</td>
</tr>
<tr>
<td>test copper-port tdr</td>
<td>Regarding cable lengths.</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

**show copper-ports tdr**

Use the `show copper-ports tdr` command to display the stored information regarding cable lengths.

**Syntax**

`show copper-ports tdr [interface]

- interface — A valid Ethernet interface identifier.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The copper-related commands do not apply to the stacking or 10GBaseT ports.

The maximum length of the cable for the Time Domain Reflectometry (TDR) test is 120 meters. Disable green-mode on the port in order to obtain accurate results.

**Example**

The following example displays the last TDR tests on all ports.

```
console#show copper-ports tdr
Port     Result                      Length [meters] Date
--------- --------------------------- --------------- ---------------------
```
show fiber-ports optical-transceiver

Use the show fiber-ports optical-transceiver command to display the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [interface]

- interface — A valid SFP, XFP or SFP+ port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The show fiber ports command is applicable to all fiber ports, including SFP, SFP+, and XFP ports. It will display an error if executed against a copper port or passive or active direct attach cables.

Examples

The following examples display the optical transceiver diagnostics.

core#show fiber-ports optical-transceiver
Output Input
Port Temp Voltage Current Power Power TX LOS
[C] [Volt] [mA] [dBm] [dBm] Fault
--------- ---- ------- ------- ------- ----- ---
Te2/0/23 22.5 3.296 7.5 -2.184 -36.990 No Yes
**test copper-port tdr**

Use the **test copper-port tdr** command to diagnose with Time Domain Reflectometry (TDR) technology the quality and characteristics of a copper cable attached to a 1GBaseT or 10GBaseT port.

**Syntax**

test copper-port tdr interface

• interface — A valid Ethernet port.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines.**

This command prompts the user to shut down the port for the duration of the test. Passive or active direct attach SFP/SFP+ cables are not based on 1000BaseT technology and do not support TDR testing. Use the **show copper-ports tdr** command to view the test results.

- The maximum distance the Virtual Cable Tester (VCT) can measure is 120 meters. Multi-gig ports (2.5G and 5G) must have the cable disconnected at the switch for the test to yield correct results. Disable green-mode on the port to ensure accurate results.

**Examples**

The following example results in a report on the cable attached to port 1/0/3.

crsh#test copper-port tdr te1/0/1

This command takes the port offline to measure the cable length. Use the show copper-port tdr command to view the results..

Do you wish to continue and take the port offline (Y/N)?y

The following example results in a failure to report on the cable attached to port te2/0/3.
console#test copper-port tdr te2/0/3

This command takes the port offline to measure the cable length. Use the show copper-port tdr command to view the results.

Do you wish to continue and take the port offline? (y/n) y

Error! Invalid interface 2/0/3
Power Over Ethernet Commands

The Dell EMC Networking PoE solution implements the PoE+ specification (IEEE 802.3at) for power sourcing equipment (PSE). IEEE 802.3at allows power to be supplied to Class 4 PD devices that require power up to 34.2 Watts. This allows the PoE+ enabled network switches and routers to be used for deployment with devices that require more power than the 802.3AF specification allows. PoE+ 802.3at is compatible with 802.3AF.

The Dell EMC Networking N3024P/N3048P switches support delivery of up to 62W of power on the first 12 interfaces of each stack unit. The Dell EMC Networking N2128PX-ON supports PoE 60W on the four 2.5G interfaces. The Dell EMC Networking N3132PX-ON supports PoE 60W on all copper ports.

- **NOTE:** This section applies to the N1108P-ON/N1124P-ON/N1148P-ON/N1524P/N1548P/N2024P/N2048P/N2128PX-ON/N3024P/N3048P/N3132PX-ON switches.

Flexible Power Management

The Dell EMC Networking PoE solution provides power management which supports power reservation, power prioritization and power limiting. The operator can assign a priority to each PoE port. When the power budget of the PoE switch has been exhausted, the higher priority ports are given preference over the lower priority ports. Lower priority ports are forcibly stopped to supply power in order to provide power to higher priority ports.

The static power management feature allows operators to reserve a guaranteed amount of power for a PoE port. This is useful for powering up devices which draw variable amounts of power and provide them an assured power range within which to operate. Class based power management allocates power at class limits as opposed to user defined limits.

In the Dynamic Power management feature, power is not reserved for a given port at any point of time. The power available with the PoE switch is calculated by subtracting the instantaneous power drawn by all the ports from the maximum available power. Thus, more ports can be powered at the same time. This feature is useful to efficiently power up more devices when the available power with the PoE switch is limited.
The Dell EMC Networking PoE solution also provides a global usage
threshold feature in order to limit the PoE switch from reaching an overload
condition. The operator can specify the limit as a percentage of the
maximum power.

**NOTE:** PoE commands are only applicable to copper ports.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>power inline</td>
<td>power inline priority</td>
<td>power inline detection</td>
<td>power inline reset</td>
<td>power inline usage-threshold</td>
</tr>
<tr>
<td>power inline four-pair forced</td>
<td>power inline management</td>
<td>clear power inline statistics</td>
<td>power inline powered-device</td>
<td>show power inline</td>
</tr>
<tr>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>show power inline firmware-version</td>
</tr>
</tbody>
</table>

**power inline**

The `power inline` command enables/disables the ability of the port to deliver
power.

**Syntax**

```plaintext
power inline {auto|never}
no power inline
```

**Command Mode**

Interface Configuration (Ethernet).
**User Guidelines**

Auto enables the switch to deliver power to the powered device. The power inline management parameter should be set to class-based mode to enable power negotiation via LLDP-MED. Dell EMC Networking PoE-enabled ports should not be connected to other Power Sourcing Equipment (PSE) with PoE enabled. If the switch detects PSE equipment supplying power to a port, PoE power is disabled on the port. If a port supplying power issues an input power detected (0x24) status and no device is attached, the port should not be used as a possible short may exist.

**Default Value**

The default value is auto, that is, device discovery is enabled and the port is capable of delivering power.

**Examples**

console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)# power inline auto

**power inline detection**

Use the `power inline detection` command to configure the detection type that tells which types of PD’s will be detected and powered by the switch. Use the `no` form of this command to set the detection type to the default.

**Syntax**

`power inline detection [unit unit-id] {dot3at | dot3at+legacy}`

`no power inline detection`

- **dot3at**—IEEE 802.3at 4-point detection only.
- **dot3at+legacy**—IEEE 802.3at 4-point detection followed by legacy capacitive detection.
- **unit unit-id**—The specific stack member to be configured.

**Default Configuration**

The default value is `dot3at+legacy`. 
**Command Mode**
Global Configuration mode

**User Guidelines**
If no unit number is specified, the entire stack is configured. If the detection mode is configured at dot3at, class-based allocation will reserve the full amount of power (33W). To use legacy 802.3af allocation, configure detection as dot3at+legacy.

**Command History**
Release 6.3.6 deprecates the legacy-only parameter in favor of dot3at+legacy as the legacy-only capability is not present in the hardware.

**power inline four-pair forced**
Use this command to force 4-pair power feed on an interface. Use the no form of the command to use the default 2-pair power feed.

**Syntax**
```
power inline four-pair forced
no power inline four-pair forced
```

**Default Configuration**
The default power feed is 2-pair power.

**Command Mode**
Interface Config

**User Guidelines**
This command is only operational on N2100PX-ON, N3000P, N3100PX-ON series switches. Only use this command when the interface is connected to a device that can accept power on all four pairs of wires (that is, on both the signal and spare pairs). Class D or better cabling is required for feeds in excess of 34.2W.

Four pair power is supported in all management modes.
• In class mode, the port limit is twice the class power.
• In dynamic mode, up to 62W may be delivered.
• In static mode, the port is limited to the configured limit.

Use this command only with devices that require up to 60W of power.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

This example configures forced 60W 4-pair power mode on interface Gi1/0/1

```
console#configure
console(config)#power inline management static
console(config)#interface gi/10/1
console(config-if-Gi1/0/1)#power inline four-pair forced
```

**power inline limit**

Use the `power inline limit` command to configure a specific power limit for a port. Use the `no` form of this command to set the power limit to the default.

**Syntax**

```
power inline limit user-defined limit
no power inline limit
```

**Default Configuration**

In two-pair mode, the default power limit is 32000 milliwatts. In four-pair mode, the default power limit is 57000 milliwatts.

**Command Mode**

Interface Configuration
User Guidelines

User defined limits are only operational if the power management mode is configured as static. By default, the power management mode is dynamic. If the operator attempts to set a user-defined limit and the power management mode is not configured as static, a warning is issued. On systems that support four-pair power, the UI does not check the limit against the port capability or the configuration. To deliver 60W power, ensure that the port is configured in four-pair mode.

The maximum configurable power limit is 32000 milliwatts for two-pair power. The maximum configurable power limit is 57000 milliwatts for four-pair power. The actual power delivered in two-pair or four-pair mode may exceed the user defined limit by up to 5%. In four-pair static mode, the maximum power delivery is approximately 59850 milliwatts (60W). Four pair power is available in any of the power management modes. In class mode, twice the detected class power is delivered (64W). In dynamic mode, up to 62W may be delivered.

The Dell EMC Networking 3024P/N3048P switches implement 4-pair PoE 60W on the first 12 lowest numbered 1G ports. The N3132PX-ON switches implement PoE 60W on the copper 1G and 5G ports. The N2128PX-ON switches implement PoE 60W on the 2.5G ports.

The lower numbered Dell EMC Networking N1108P/N1124P/N1148P front-panel copper ports support PoE (15.4W) and PoE+ (34.2W) as well as legacy capacitive detection for pre-standard powered devices (PDs). The N1108P supports PoE on ports 1-4 or any two of the ports may supply PoE+ power. The N1124P supports PoE on ports 5-16 or any six of the ports may supply PoE+ power. The N1148P supports PoE on ports 1-24 or any twelve of the ports may supply PoE+ power.

Example

This example configures interface Gi1/0/1 to deliver 60W four-pair power.

```console
console#configure
console(config)#power inline management static
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#power inline four-pair forced
```

This example configures interface Gi1/0/2 to deliver 50W four-pair power (within the 5% tolerance). The port will deliver up to 52500 mW.

```console
console#configure
```
console(config)#power inline management static
console(config)#interface gi1/0/2
console(config-if-Gi1/0/2)#power inline four-pair forced
console(config-if-Gi1/0/2)#power inline limit user-defined 50000

This example displays an interface configured in four-pair power mode.

console#show power inline gigabitethernet 1/0/1 detailed

<table>
<thead>
<tr>
<th>Port</th>
<th>Powered Device</th>
<th>State</th>
<th>Priority</th>
<th>Status</th>
<th>Class</th>
<th>Power [mW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Limit</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>None</td>
<td>57000</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Overload Counter ........................................ 0
Short Counter ........................................... 0
Denied Counter .......................................... 0
Absent Counter ........................................... 0
Invalid Signature Counter ................................ 0
Output Volts ............................................ 53
Output Current .......................................... 0
Temperature ............................................. 49

**Command History**

Description revised in 6.3.5 release.

**power inline management**

Use the `power inline management` command in Global Configuration mode to set the power management type. This command is used along with the `power inline priority` command. Use the `no` form of this command to set the management mode to the default.

**Syntax**

`power inline management [unit unit-id] {dynamic | static | class}`

`no power inline management [unit unit-id]`

- `dynamic`—Dynamic power management
• **static**—Static power management
• **class**—Class-based power management
• **unit-id**—A stack unit ID.

**Default Configuration**
Default management is dynamic.

**Command Mode**
Global Configuration

**User Guidelines**
If no unit is specified, all members of the stack are configured. Static, dynamic and class-based modes differ in how the available power is calculated and how much power may be delivered to the Powered Device. Refer to the PoE section in the User’s Configuration Guide for information on Powered Device detection, power allocation methods, and the PoE guard band.

**Example**
In the following example, no port is specified so the command displays global configuration and status of all the ports. Configure the global power management scheme as dynamic with dot3at+legacy detection and enable PoE capability on ports Gi1/0/1-10.

```
console(config)#power inline management dynamic
console(config)#power inline detection dot3at+legacy
console(config)#interface range Gi1/0/1-10
console(config-if)#power inline auto
console(config-if)#exit
console#show power inline
Unit Status
============
Unit........................................... 1
Power.......................................... On
Total Power.................................... 500 Watts
Threshold Power............................... 450 Watts
Consumed Power............................... 0 Watts
Usage Threshold.............................. 90%
Power Management Mode...................... Dynamic
Power Detection Mode......................... dot3at+legacy
```
Port Configuration
==================

<table>
<thead>
<tr>
<th>Port</th>
<th>Powered Device</th>
<th>State</th>
<th>Priority</th>
<th>Status</th>
<th>Class</th>
<th>Power [mW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td></td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td></td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td></td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td></td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

Command History
Description revised in version 6.3.1.5 release.
Description revised in version 6.3.1.6 release. Example revised in 6.4 release.

**power inline powered-device**

The **power inline powered-device** command adds a comment or description of the powered device type to enable the user to remember what is attached to the interface. To remove the description, use the no form of this command.

**Syntax**

derived from

```
power inline powered-device pd-type
do  power inline powered-device

• pd-type — Specifies the type of powered device attached to the interface. (Range: 1–20 characters)
```

**Command Mode**
Interface Configuration (Ethernet).

**User Guidelines**
No specific guidelines.

**Examples**

```
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)# power inline powered-device IP-phone
```
power inline priority

The `power inline priority` command configures the port priority level, for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower-numbered port has higher priority.

For a system delivering peak power to a certain number of devices, if a new device is attached to a high-priority port, power to a low-priority port is shut down and the new device is powered up.

**Syntax**

```plaintext
power inline priority {critical | high | low}
no power inline priority
```

**Command Mode**

Interface Configuration (Ethernet).

**User Guidelines**

Priority is always enabled for all ports. If all ports have equal priority in an overload condition, the switch will shut down the highest numbered ports first.

**Default Value**

`Low`

**Examples**

```plaintext
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)# power inline priority high
```

power inline reset

Use the `power inline reset` command to reset the port.
**Syntax**

power inline reset

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration

**User Guidelines**

This command is useful if the port is stuck in an Error state. Power to the powered devices may be interrupted as the port is reset.

**power inline usage-threshold**

The `power inline usage-threshold` command configures the system power usage threshold level at which lower priority ports are disconnected. The threshold is configured as a percentage of the total available power. Use the `no` form of the command to set the threshold to the default value.

**Syntax**

```
power inline usage-threshold [unit unit-id] threshold
no power inline usage-threshold [unit unit-id]
```

- **threshold**— Power threshold at which ports are disconnected. The range is 25-99%.
- **unit-id**— A stack member identifier.

**Default Configuration**

The default threshold is 90%.

**Command Mode**

Global Configuration.
User Guidelines
If no unit number is specified, all stack members are configured. The power limit beyond which ports are disconnected has a configurable range as a percentage of total available power for the individual unit. The maximum power available is given in the table shown in the power inline management command. The usage threshold check calculates the actual consumed power and compares it against the (unit power maximum multiplied by the threshold)/100. If unit power consumption exceeds the threshold, and the power bank is active, ports are disconnected with an over-power condition. The disconnection is priority based. When ports are disconnected due to actual consumed power exceeding the threshold, a trap is generated.

Examples
console(config)# power inline usage-threshold 90

Command History
Syntax updated in 6.4 release.

clear power inline statistics
Use this command to clear the PoE statistics.

Syntax
clear power inline statistics [interface-id]
  •  interface-id—An Ethernet interface capable of supplying PoE power.

Default Configuration
This command has no default configuration.

Command Modes
Privileged Exec

User Guidelines
If no interface is specified, the statistics are cleared for all PoE-capable interfaces.
**show power inline**

Use the `show power inline` command to report current PoE configuration and status. If no port is specified, the command displays global configuration and status of all the ports. If a port is specified, then the command displays the details for the single port. Use the detailed parameter to show power limits, detection type and high power mode for the interface.

**Syntax**

```
show power inline [interface-id] [detailed]
```

- `interface-id`—Any PoE-capable Ethernet interface. See Interface Naming Conventions for interface representation.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Ports configured in static mode will always show as Class 0 regardless of the actual PD type.

The Power column shows the actual power drawn, not the configured value.

If a port supplying power detects PSE equipment, the power to the port is shut off. If a powered port shows input power detected status (0x24), and no device is attached, the port should not be used as a possible short may exist.

The PoE controller returns the Total Power Consumed value in Watts. For this reason, Total Power Consumption value displayed might not exactly match the sum of power in milliwatts consumed by various Powered Devices.

**Examples**

In the next example, the port is specified and the command displays the configuration and status for the specified port.

```
console#show power inline gigabitethernet 1/0/13
Port    Powered Device   State Priority  Status    Class[W]  Power[mW]
------   --------------- -----  --------  --------- -------------- ------
Gi1/0/13                Auto   Low       On        3.84 - 6.49   5000

Overload Counter............................... 0
```
In the next example, the port is specified and the command displays the details for the single port. The detected class and power is shown, followed by the power limit configuration. Then port counters, voltage, current and temperate are displayed.

```
cable#show power inline gi1/0/1 detailed

<table>
<thead>
<tr>
<th>Port</th>
<th>Powered Device</th>
<th>State</th>
<th>Priority</th>
<th>Status</th>
<th>Class</th>
<th>Power[mW]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/0/13</td>
<td></td>
<td>auto</td>
<td>Low</td>
<td>Searching</td>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Limit</th>
<th>Power</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/0/13</td>
<td>None</td>
<td>32000</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

Overload Counter............................... 0
Short Counter.................................. 0
Denied Counter................................. 0
Absent Counter................................. 0
Invalid Signature Counter...................... 0
Output Volts................................... 53
Output Current................................. 0
Temperature.................................... 38

Command History
Example updated in 6.4 release.

**show power inline firmware-version**

Use the `show power inline firmware-version` command to display the version of the PoE controller firmware present on the switch file system.

**Syntax**

```
show power inline firmware-version
```
**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command displays the PoE firmware version for each stack member individually.

**Example**

```
console(config)#show power inline firmware-version
Unit       Firmware Version
----       ----------------
1         265_1
```
RMON Commands

The Dell EMC Networking SNMP component includes an RMON (remote monitoring) agent. RMON is a base technology used by network management applications to manage a network. Troubleshooting and network planning can be accomplished through the network management applications. The network monitor monitors traffic on a network and records selected portions of the network traffic and statistics. The collected traffic and statistics are retrieved using SNMP. The data collected is defined in the RMON MIB, RFC 2819. A device that supports gathering and reporting the RMON data is referred to as an RMON probe or RMON Agent. An RMON probe provides RMON data to an RMON Manager for analysis and presentation to the user. An RMON probe may be embedded in an existing network device or stand-alone.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>rmon alarm</th>
<th>show rmon collection history</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon collection history</td>
<td>show rmon events</td>
</tr>
<tr>
<td>rmon event</td>
<td>show rmon hcalarm</td>
</tr>
<tr>
<td>rmon hcalarm</td>
<td>show rmon history</td>
</tr>
<tr>
<td>show rmon alarm</td>
<td>show rmon log</td>
</tr>
<tr>
<td>show rmon alarms</td>
<td>show rmon statistics</td>
</tr>
</tbody>
</table>

rmon alarm

Use the rmon alarm command in Global Configuration mode to configure alarm conditions. To remove an alarm, use the no form of this command. See also the related show rmon alarm command.

Syntax

rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string] [startup direction]
no rmon alarm number

- number—The alarm index. (Range: 1–65535)
- variable—A fully qualified SNMP object identifier that resolves to a particular instance of a MIB object.
- interval—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1–2147483647)
- rising-threshold value—Rising Threshold value. (Range: -2147483648 – 2147483647)
- falling-threshold value—Falling Threshold value. (Range: -2147483648 – 2147483647)
- event-number—The index of the Event that is used when a rising or falling threshold is crossed. (Range: 1-65535)
- delta—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is delta, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.
- absolute—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.
- startup direction—The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the rising-threshold, and direction is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the falling-threshold, and direction is equal to falling or rising-falling, then a single falling alarm is generated.
- owner string—Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

Default Configuration
No alarms are configured.

Command Mode
Global Configuration mode
User Guidelines

This command has no user guidelines.

Example

The following example configures the following alarm conditions:

- Alarm index — 1
- Variable identifier — 1.3.6.1.2.1.2.2.1.10.5
- Sample interval — 10 seconds
- Rising threshold — 500000
- Falling threshold — 10
- Rising threshold event index — 1
- Falling threshold event index — 1

```
console(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.10.5 10 500000 10 1 1
```

rmon collection history

Use the `rmon collection history` command in Interface Configuration mode to enable a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the `no` form of this command. Also see the `show rmon collection history` command.

Syntax

```
rmon collection history index [owner ownername] [buckets bucket-number] [interval seconds]
```

```
no rmon collection history index
```

- `index` — The requested statistics index group. (Range: 1–65535)
- `owner ownername` — Records the RMON statistics group owner name. If unspecified, the name is an empty string.
- `buckets bucket-number` — A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 65535)
- `interval seconds` — The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1–3600)
Default Configuration
The buckets configuration is 50. The interval configuration is 1800 seconds.

Command Mode
Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode.

User Guidelines
This command cannot be executed on multiple ports using the interface range command.

Example
The following example enables a Remote Monitoring (RMON) MIB history statistics group on port 1/0/8 with the index number “1” and a polling interval period of 2400 seconds.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-Gi1/0/8)#rmon collection history 1 interval 2400
```

rmon event
Use the rmon event command in Global Configuration mode to configure an event. To remove an event, use the no form of this command. See also the show rmon events command.

Syntax
```
rmon event number [log] [trap community] [description string] [owner string]
no rmon event number
```
- **number**—The event index. (Range: 1–65535)
- **log**—An entry is made in the log table for each event.
- **trap**—An SNMP trap is sent to one or more management stations.
- **community**—If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description**—A comment describing this event. (Range 0-127 characters)
• **owner**—Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
The following example configures an event with the trap index of 10.
```
console(config)#rmon event 10 log
```

**rmon hcalarm**
Use the `rmon hcalarm` to configure high capacity alarms. Use the `no` form of the command to remove the alarm.

**Syntax**
```
rmon hcalarm alarmnumber variable interval {absolute | delta} rising-threshold value-64[rising-event-index] falling-threshold value-64[falling-event-index] [startup {rising | falling | rising-falling}] [owner string]
```

- **alarmnumber**—An alarm number that uniquely identifies the alarm entry. (Range: 1-65536). Each entry defines a diagnostic sampler at a particular interval for an object on the device.
- **variable**—The MIB object to monitor. May be fully qualified or relative. Only variables that resolve to an ASN.1 primitive type of INTEGER are allowed.
- **interval**—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1–2147483647. The default is 1 second.)
• **absolute**—Specifies to use a fixed value for the threshold (Default value).

• **delta**—Specifies to use the difference between the current value and the previous value.

• **rising-threshold** value-64—Rising threshold value \((-2^{63}) \text{ to } 2^{63} - 1\)

• **rising-event-index**—Event to trigger when the rising threshold is crossed (1–65535).

• **falling-threshold-high** value-64—Falling threshold value \((-2^{63}) \text{ to } 2^{63} - 1\)

• **falling-event-index**—Event to trigger when the rising threshold is crossed (1–65535).

• **startup** \{rising|falling|rising-falling\}—The event that is sent when this entry is first set to active. If the first sample after this entry is configured is greater than or equal to the rising threshold and startup rising or startup rising-falling is configured, a single rising event is generated. If the first sample after this entry is configured is less than or equal to the falling threshold and startup falling or startup rising-falling is configured then a single falling event is generated.

• **owner** string—Specify an owner for the alarm (string – no default).

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command has no user guidelines.

**Example**
```
console(config)# rmon hcalarm 2 ifInOctets.1 30 absolute rising-threshold high 2147483648 falling-threshold high -2147483648 startup rising owner “dell-owner”
```
**show rmon alarm**

Use the `show rmon alarm` command in User Exec mode to display alarm configuration. Also see the `rmon alarm` command.

**Syntax**

```
show rmon alarm number
```

- number — Alarm index. (Range: 1–65535)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays RMON 1 alarms.

```
console> show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Alarm index.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Last Sample Value</td>
<td>The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>The method of sampling the variable and calculating the value compared against the thresholds. If the value is <code>absolute</code>, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is <code>delta</code>, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</td>
</tr>
<tr>
<td>Startup Alarm</td>
<td>The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.</td>
</tr>
<tr>
<td>Rising Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Falling Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Rising Event</td>
<td>The event index used when a rising threshold is crossed.</td>
</tr>
<tr>
<td>Falling Event</td>
<td>The event index used when a falling threshold is crossed.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
show rmon alarms

Use the show rmon alarms command in User Exec mode to display the alarms summary table.

Syntax

show rmon alarms

Default Configuration

This command has no arguments or keywords.

Command Mode

User Exec, Privileged Exec modes, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays the alarms summary table:

```
console> show rmon alarms
Index   OID                     Owner
-----   ----------------------  -------
1       1.3.6.1.2.1.2.2.1.10.1  CLI
2       1.3.6.1.2.1.2.2.1.10.1  Manager
3       1.3.6.1.2.1.2.2.1.10.9  CLI
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
show rmon collection history

Use the show rmon collection history command in User Exec mode to display the requested group of statistics. Also see the rmon collection history command.

Syntax

show rmon collection history [{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}]

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The sampled Ethernet interface.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds between samples.</td>
</tr>
<tr>
<td>Requested Samples</td>
<td>The requested number of samples to be saved.</td>
</tr>
<tr>
<td>Granted Samples</td>
<td>The granted number of samples to be saved.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

Example

The following example displays all RMON group statistics.

console> show rmon collection history
Index  Interface  Interval  Requested  Granted  Owner
Samples  Samples

----------------------------------------------------------------------------
show rmon events

Use the `show rmon events` command in User Exec mode to display the RMON event table. Also see the `rmon event` command.

**Syntax**

`show rmon events`

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of notification that the device generates about this event. Can have the following values: none, log, trap, log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.</td>
</tr>
<tr>
<td>Community</td>
<td>If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this event.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The time this entry last generated an event. If this entry has not generated any events, this value is zero.</td>
</tr>
</tbody>
</table>
Example

The following example displays the RMON event table.

```
console> show rmon events
Index Description   Type    Community   Owner     Last time sent
-----  -----------   ----   ---------   ------  -------------------
1      Errors       Log     CLI         Jan 18 2005 23:58:17
2      High Broadcast Log-Trap  switch  Manager Jan 18 2005 23:59:48
```

show rmon hcalarm

Use the show rmon hcalarm command to display high capacity (64-bit) alarms configured with the `rmon hcalarm` command.

Syntax

```
show rmon {hcalarms | hcalarm number}
```

- `number`—The alarm index (Range: 1-65535)

Default Configuration

This command has no default configuration.

Command Modes

Privileged Exec (all show modes)

User Guidelines

This command has no user guidelines.

Example

```
console#show rmon hcalarm 2

Alarm 2
-------
OID: ifInOctets.1
Last Sample Value: 0
Interval: 30
Sample Type: absolute
Startup Alarm: rising
Rising Threshold High: 2
Rising Threshold Low: 10
```
Rising Threshold Status: Positive
Falling Threshold High: 20
Falling Threshold Low: 10
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising
Owner: dell-owner

cconsole#show rmon hcalarms

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ifInOctets.1</td>
<td>dell-owner</td>
</tr>
</tbody>
</table>

**show rmon history**

Use the **show rmon history** command in User Exec mode to display RMON Ethernet Statistics history. Also see the **rmon collection history** command.

**Syntax**

```
show rmon history [index [throughput | errors | other] [period seconds]]
```

- **index** — The requested set of samples. (Range: 1–65535)
- **throughput** — Displays throughput counters.
- **errors** — Displays error counters.
- **other** — Displays drop and collision counters.
- **period seconds** — Specifies the requested period time to display. (Range: 0–2147483647)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table describes the significant fields shown in the display:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and Time the entry is recorded.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>The number of packets (including bad packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The number of good packets received during this sampling interval that were directed to the Broadcast address.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the Broadcast address.</td>
</tr>
<tr>
<td>%</td>
<td>The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>CRC Align</td>
<td>The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize</td>
<td>The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Oversize</td>
<td>The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
</tbody>
</table>
Examples

The following example displays RMON Ethernet Statistics history for “throughput” on index number 1.

```
console> show rmon history 1 throughput
Sample Set: 1 Owner: CLI
Interface: Gi1/0/1 interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 270

<table>
<thead>
<tr>
<th>Time</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>09-Mar-2005</td>
<td>18:29:32</td>
<td>303595962</td>
<td>357568</td>
<td>3289</td>
<td>7287 19</td>
</tr>
<tr>
<td>09-Mar-2005</td>
<td>18:29:42</td>
<td>287696304</td>
<td>275686</td>
<td>2789</td>
<td>5878 20</td>
</tr>
</tbody>
</table>
```

The following example displays RMON Ethernet Statistics history for errors on index number 1.

```
console> show rmon history 1 errors
Sample Set: 1 Owner: Me
Interface: Gi1/0/1 interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500 (800 after reset)

<table>
<thead>
<tr>
<th>Time</th>
<th>CRC</th>
<th>Undersize</th>
<th>Oversize</th>
<th>Fragments</th>
<th>Jabbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>09-Mar-2005</td>
<td>18:29:32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09-Mar-2005</td>
<td>18:29:42</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The following example displays RMON Ethernet Statistics history for “other” on index number 1.

```
```

Field | Description
--- | ---
Jabbers | The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped | The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped. It is just the number of times this condition has been detected.
Collisions | The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.
console> show rmon history 1 other
Sample Set: 1               Owner: Me
Interface:  Gi1/0/1 Interval: 1800
Requested samples: 50       Granted samples: 50
Maximum table size: 270

<table>
<thead>
<tr>
<th>Time</th>
<th>Dropped</th>
<th>Collisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-Mar-2005 22:06:00</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>10-Mar-2005 22:06:20</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

**show rmon log**

Use the `show rmon log` command in User Exec mode to display the RMON logging table.

**Syntax**

`show rmon log [event]`

- `event` — Event index. (Range: 1–65535)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Time</td>
<td>The time this entry was created.</td>
</tr>
</tbody>
</table>

**Example**

The following examples display the RMON logging table.
console> show rmon log
Maximum table size: 100
Event Description     Time
----- -----------     --------------------
1     Errors          Jan 18 2005  23:48:19
1     Errors          Jan 18 2005  23:58:17
2     High Broadcast  Jan 18 2005  23:59:48
console> show rmon log
Maximum table size: 100 (100 after reset)
Event Description     Time
----- -----------     --------------------
1     Errors          Jan 18 2005  23:48:19
1     Errors          Jan 18 2005  23:58:17
2     High Broadcast  Jan 18 2005  23:59:48

show rmon statistics

Use the show rmon statistics command in User Exec mode to display the RMON Ethernet Statistics.

Syntax

show rmon statistics {gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following table describes the significant fields shown in the display:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped</td>
<td>The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The total number of good packets received and directed to the Broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The total number of good packets received and directed to a multicast address. This number does not include packets directed to the Broadcast address.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
</tbody>
</table>
### Example

The following example displays RMON Ethernet Statistics for port Te1/0/1.

```console
console#show rmon statistics tengigabitethernet 1/0/1
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>64 Octets</td>
<td>The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>65 to 127 Octets</td>
<td>The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255 Octets</td>
<td>The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256 to 511 Octets</td>
<td>The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512 to 1023 Octets</td>
<td>The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024 to 1518 Octets</td>
<td>The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>HC Overflow Pkts 65 - 127 Octets: 0</td>
<td>HC Pkts 65 - 127 Octets: 0</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>HC Overflow Pkts 128 - 255 Octets: 0</td>
<td>HC Pkts 128 - 255 Octets: 0</td>
</tr>
<tr>
<td>HC Overflow Pkts 256 - 511 Octets: 0</td>
<td>HC Pkts 256 - 511 Octets: 0</td>
</tr>
<tr>
<td>HC Overflow Pkts 512 - 1023 Octets: 0</td>
<td>HC Pkts 512 - 1023 Octets: 0</td>
</tr>
<tr>
<td>HC Overflow Pkts 1024 - 1518 Octets: 0</td>
<td>HC Pkts 1024 - 1518 Octets: 0</td>
</tr>
</tbody>
</table>
Serviceability Commands

Debug commands cause the output of the enabled trace to display on a serial port or telnet console. Note that the output resulting from enabling a debug trace always displays on the serial port. The output resulting from enabling a debug trace displays on all login sessions for which any debug trace has been enabled. The configuration of a debug command remains in effect the whole login session.

The output of a debug command is always submitted to the SYSLOG service at a DEBUG severity level. As such, it can be forwarded to a SYSLOG server, stored in the buffer log, or otherwise processed in accordance with the configuration of the SYSLOG service. Configuration of console logging in the SYSLOG service is not required in order to view the output of debug traces.

Debug commands are provided in the normal CLI tree. Debug settings are not persistent and are not visible in the running configuration. To view the current debug settings, use the `show debugging` command.

The output of debug commands can be large and may adversely affect system performance.

Enabling debug for all IP packets can cause a serious impact on the system performance; therefore, it is limited by ACLs. This means debug can be enabled for IP packets that conform to the configured ACL. This also limits the feature availability to only when the QoS component is available. Debug for VRRP and ARP are available on routing builds.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command 1</th>
<th>Command 2</th>
<th>Command 3</th>
<th>Command 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug aaa accounting</td>
<td>debug igmp snooping</td>
<td>debug ipv6 pim sm</td>
<td>exception core-file</td>
</tr>
<tr>
<td>debug arp</td>
<td>debug ip acl</td>
<td>debug isdp</td>
<td>exception dump</td>
</tr>
<tr>
<td>debug authentication</td>
<td>debug ip bgp</td>
<td>debug lacp</td>
<td>exception protocol</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>debug auto-voip</td>
<td>debug ip dvmrp</td>
<td>debug mldsnooping</td>
<td>exception switch-chip-register</td>
</tr>
</tbody>
</table>
**NOTE:** Debug commands are not persistent across resets.

### debug aaa accounting

Use the `debug aaa accounting` command to enable debugging for accounting. Use the `no` form of the command to disable accounting debugging.

**Syntax**

d debug aaa accounting  
no debug aaa accounting

**Default Configuration**

Debugging is disabled by default.

**Command Mode**

Privileged Exec mode
**User Guidelines**
Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

**Example**
```
console#debug aaa accounting
```

**debug arp**
Use the `debug arp` command to enable tracing of ARP packets. Use the `no` form of this command to disable tracing of ARP packets.

Use of the optional `vrf` parameter executes the command within the context of the VRF specific routing table.

**Syntax**
```
ddebug arp [vrf vrf-name]
no debug arp
```
- **vrf-name**—The name of the VRF associated with the routing table context used by the command. If no vrf is specified, the global routing table context is used.

**Default Configuration**
ARP packet tracing is disabled by default.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the vrf parameter.

This vrf parameter is only available on the N3000/N3100/N4000 switches.
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console# debug arp
```

### debug authentication interface

Use this command to enable Authentication Manager debug traces for the interface. Use the **no** form of this command to set the debug trace to factory default value.

#### Syntax

```
debug authentication {event | all} interface-id
```

```
no debug authentication {event | all} interface-id
```

- **event**—Traces Authentication Manager debug events.
- **all**—Enables all Authentication Manager debugs.
- **interface-id**—The interface to trace.

#### Default Configuration

Default value is disabled.

#### Command Modes

Privileged Exec mode

#### User Guidelines

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console# debug authentication event Gi1/0/1
console# debug authentication all Gi1/0/1
```
**debug auto-voip**

Use the **debug auto-voip** command to enable Auto VOIP debug messages. See the optional parameters to trace H323, SCCP, or SIP packets respectively. Use the “no” form of this command to disable Auto VOIP debug messages.

**Syntax**

depug auto-voip [H323 | SCCP | SIP]

no debug auto-voip [H323 | SCCP | SIP]

**Default Configuration**

Auto VOIP tracing is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

crsole#debug auto-voip

**debug bfd**

Use this command to enable the display of BFD events or packets.

**Syntax**

depug bfd {packet | event}

no debug bfd {packet | event}

- packet—Display BFD control packets.
- event—Display BFD state transition events.
**Default Configuration**
Debug is disabled by default.

**Command Mode**
Privileged Exec

**User Guidelines**
Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

**Example**
```
console# configure
console(config)# vlan 100
console(config-vlan100)# exit
console(config)# interface vlan 100
console(config-if-vlan100)# bfd interval 100 min_rx 100 multiplier 5
```

**debug cfm**
Use the `debug cfm` command to enable CFM debugging. Use the `no` form of the command to disable debugging.

**Syntax**
```
default cfm {event | {pdu {all | ccm | ltm | lbm |} {tx | rx}}}
```
- **event**—CFM events
- **pdu**—CFM PDUs
- **ccm**—Continuity check messages
- **ltm**—Link trace messages
- **lbm**—Loopback messages
- **tx**—Transmit only
- **rx**—Receive only
- **all**—Everything
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec

User Guidelines
Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

Example
The following examples enables display of CFM events on the console.
console#debug cfm event

d debug clear
Use the debug clear command to disable all debug traces.

Syntax
d debug clear

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode.

User Guidelines
There are no user guidelines for this command.

Example
console#debug clear
**debug console**

Use the **debug console** to enable the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands appears on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

**Syntax**

ddebug console

**Default Configuration**

Display of debug traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

cconsole#debug console

ddebug crashlog

Use this command to display the crash log contents on the console.

**Syntax**

ddebug crashlog {crashlog-index | proc | kernel crashlog-index | data crashlog-index [comp-id] [item-number] [add-param] [add-param] | deleteall} [unit unit-index]

- crashlog-index—Indicates which crash log to display. The range is 0-4. 0 indicates the most recent log and 4 specifies the oldest log.
• **proc**—Display the process crash log.
• **kernel**—Display the kernel crash data.
• **data**—Display the crash summary data.
• **deleteall**—Delete all existing crash logs.
• **unit-index**—An optional specifier identifying the stack unit number from which to obtain the crash log.
• **comp-id**—
• **item-number**—
• **add-param**—

**Default Configuration**
By default, this command displays all crash logs for the specified index.

**Command Modes**
Privileged Exec mode, User Config mode, all show modes

**User Guidelines**
There are no user guidelines for this command.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
This example displays the most recent crash log for the stack master.

```
console#debug crashlog 0

Displaying Crash Dump 0
For kernel Crash Dump - osapiDebugCrashDumpDisplay(x,1)

********************************************************************
*       Start Stack Information       *
********************************************************************
pid:            32195
TID:            -1215952016
Task Name:      emWeb
si_signo:       11
si_errno:       0
```
si_code: 1
si_addr: 0x0
Date/Time: 8/13/2011 16:37:31
SW ver: 0.0.0.0

---------- CALL STACK INFO ----------
Stack pointer before signal: 0x00000000
Offending instruction at address 0x00000000
tried to access address 0x00000000
CPU's exception-cause code: 0x00000000
Registers (hex) at time of fault:
    r01: 00000000 r02: 00000000 r03: 00000000 r04: 00000000
    r05: 00000000 r06: 00000000 r07: 00000000 r08: 00000000 r09: 00000000
    r10: 00000000 r11: 00000000 r12: 00000000 r13: 00000000 r14: 00000000
    r15: 00000000 r16: 00000000 r17: 00000000 r18: 00000000 r19: 00000000
    r20: 00000000 r21: 00000000 r22: 00000000 r23: 00000000 r24: 00000000
    r25: 00000000 r26: 00000000 r27: 00000000 r28: 00000000 r29: 00000000
    r30: 00000000 r31: 00000000

$0x083da883$ $0x083c9955$ $0x0804b8f6$ $0x0012e40c$ $0x083c73c3$
$0x083c7211$
$0x082b05e3$ $0x081ed66c$ $0x0839db78$ $0x083a0c22$ $0x0839b295$
$0x0839a928$
$0x083a7b73$ $0x08387592$ $0x08372fbc$ $0x08395caf$ $0x083996de$
$0x083d6f71$
$0x00134e99$ $0x0021873e$

-----------------------------------------
***************************************************
*          End Stack Information         *
***************************************************

---------- CALL STACK INFO (VERBOSE) ----------
Stack pointer before signal: 0x00000000
Offending instruction at address 0x00000000
tried to access address 0x00000000
CPU's exception-cause code: 0x00000000
Registers (hex) at time of fault:
    r01: 00000000 r02: 00000000 r03: 00000000 r04: 00000000
    r05: 00000000 r06: 00000000 r07: 00000000 r08: 00000000 r09: 00000000
    r10: 00000000 r11: 00000000 r12: 00000000 r13: 00000000 r14: 00000000
    r15: 00000000 r16: 00000000 r17: 00000000 r18: 00000000 r19: 00000000
    r20: 00000000 r21: 00000000 r22: 00000000 r23: 00000000 r24: 00000000
    r25: 00000000 r26: 00000000 r27: 00000000 r28: 00000000 r29: 00000000
    r30: 00000000 r31: 00000000

******************************************************************************
*       End Stack Information       *
******************************************************************************
debug dhcp packet

Use the `debug dhcp packet` command to display debug information about DHCPv4 client activities and to trace DHCPv4 packets to and from the local DHCPv4 client. To disable debugging, use the `no` form of this command.

**Syntax**

download dhcp packet [transmit | receive]

no debug dhcp packet [transmit | receive]

**Default Configuration**

By default, DHCP client packet tracing is disabled.

**Command Mode**

Privileged Exec
**User Guidelines**

The DHCP client has an internal packet tracing capability. This command turns the packet tracing on.

Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

**Example**

This example enables DHCP client packet tracing for both transmit and receive flows.

```
console#debug dhcp packet
```

The second example is for transmit flow.

```
console#debug dhcp packet transmit
```

The third example is for receive flow.

```
console#debug dhcp packet receive
```

**debug dhcp server packet**

Use this command to trace DHCPv4 packets to and from the local DHCPv4 server. To disable debugging, use the no form of this command.

**Syntax**

```
default dhcp server packet
no debug dhcp server packet
```

**Default Configuration**

DHCP server packet tracing is disabled by default.

**Command Mode**

Privileged Exec

**User Guidelines**

The DHCP server supports an internal packet tracing facility. This command turns the packet tracing on.
Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

Example
This example enables DHCP server packet tracing.

```
console#debug dhcp server packet
```

debug dot1ag

Use this command to enable or disable the tracing of CFM components for events and CFM PDUs based on the type of packet for reception and transmission.

Syntax

debug dot1ag {all | ccm | events | lbm | lbr | ltm | ltr | pdu}

no debug dot1ag {all | ccm | events | lbm | lbr | ltm | ltr | pdu}

- **all**—Traces CCM, LBM, LBR, LTM, LTRs.
- **ccm**—Traces CCMs
- **events**—Traces CFM events
- **lbm**—Traces LBMs
- **lbr**—Traces LBRs
- **ltm**—Traces LTMs
- **ltr**—Traces LTRs
- **pdu**—Traces specific PDUs

Default Configuration

Tracing is disabled by default.

Command Modes

Privileged Exec mode

User Guidelines

This command is only application to N4000 series switches.
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```plaintext
console#debug dot1ag all
Dot1ag CCM, LBM, LBR, LTM, LTR tracing enabled.

console#

console#debug dot1ag events
Dot1ag events tracing enabled.

console#

console#debug dot1ag ccm
Dot1ag CCM tracing enabled.

console#

console#no debug dot1ag ccm
Dot1ag CCM tracing disabled.
```

**debug dot1x**

Use the `debug dot1x` command to enable dot1x packet tracing. Use the “no” form of this command to disable dot1x packet tracing.

**Syntax**

```
depot dot1x packet [receive | transmit]
no debug dot1x packet [receive | transmit]
```

**Default Configuration**

Display of dot1x traces is disabled by default.

**Command Mode**

Privileged Exec mode.
**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console#debug dot1x packet
```

### debug igmpsnooping

Use the `debug igmpsnooping` to enable tracing of IGMP Snooping packets transmitted and/or received by the switch. IGMP Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

**Syntax**

```
debug igmpsnooping packet [receive | transmit]
no debug igmpsnooping packet [receive | transmit]
```

**Default Configuration**

Display of IGMP Snooping traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console#debug igmpsnooping packet
```
**debug ip acl**

Use the `debug ip acl` command to enable debug of IP Protocol packets matching the ACL criteria. Use the “no” form of this command to disable IP ACL debugging.

**Syntax**

```
debug ip acl acl
no debug ip acl acl
```

- `acl` — The number of the IP ACL to debug.

**Default Configuration**

Display of IP ACL traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console#debug ip acl 1
```

**debug ip bgp**

To enable debug tracing of BGP events, use the `debug ip bgp` command. To disable debug tracing, use the `no` form of this command.

**Syntax**

```
depug ip bgp [vrf vrf-name] [ipv4-address | ipv6-address [interface interface-id]] [events | keepalives | notification | open | refresh | updates | in | out]
```

```
no debug ip bgp [ipv4-address | ipv6-address [interface interface-id]] [events | keepalives | notification | open | refresh | updates | in | out]
```

- `interface-id`—A routing interface identifier (VLAN interface).
• `vrf vrf-name`—Displays aggregate address information associated with the named VRF.

• `ipv4-address`—(Optional) The IPv4 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.

• `ipv6-address [interface interface-id]`—The IPv6 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.

• `events`—(Optional) Trace adjacency state events.

• `keepalives`—(Optional) Trace transmit and receive of KEEPALIVE packets.

• `notification`—(Optional) Trace transmit and receive of NOTIFICATION packets.

• `open`—(Optional) Trace transmit and receive of OPEN packets.

• `refresh`—(Optional) Traces transmit and receive of ROUTE REFRESH packets.

• `updates`—(Optional) Traces transmit and receive of UPDATE packets.

• `in`—(Optional) Trace received packets.

• `out`—(Optional) Trace sent packets.

**Default Configuration**

Debug tracing is not enabled by default. By default, debug capability for the the global VRF is configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

Debug messages are sent to the system log at the DEBUG severity level. To print them on the console, enable console logging at the DEBUG level (`logging console debug`).

The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer.
Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

If the vrf-name is specified, information pertaining to that VRF is displayed.

**Command History**

Introduced in version 6.2.0.1 firmware.
Updated in version 6.3.0.1 firmware.

**Example**

```
console#debug ip bgp 10.27.21.142 events
d debug ip dvmrp
```

**debug ip dvmrp**

Use the `debug ip dvmrp` to trace DVMRP packet reception and transmission. The `receive` option traces only received DVMRP packets and the `transmit` option traces only transmitted DVMRP packets. When neither keyword is used in the command, all DVMRP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

**Syntax**

```
d debug ip dvmrp packet [receive | transmit]
no debug ip dvmrp packet [receive | transmit]
```

**Default Configuration**

Display of DVMRP traces is disabled by default.

**Command Mode**

Privileged Exec mode.
User Guidelines
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

Example
console#debug ip dvmrp packet

debug ip igmp
Use the debug ip igmp command to trace IGMP packet reception and transmission. The receive option traces only received IGMP packets and the transmit option traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable IGMP traces.

Syntax
debug ip igmp packet [receive | transmit]
no debug ip igmp packet [receive | transmit]

Default Configuration
Display of IGMP traces is disabled by default.

Command Mode
Privileged Exec mode.

User Guidelines
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

Example
cconsole#debug ip igmp packet
**debug ip mcache**

Use the `debug ip mcache` command for tracing MDATA packet reception and transmission. The `receive` option traces only received data packets and the `transmit` option traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable MDATA tracing.

**Syntax**

```
depth ip mcache packet [receive | transmit]
no debug ip mcache packet [receive | transmit]
```

**Default Configuration**

Display of MDATA traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console#debug ip mcache packet
```

**debug ip pimdm packet**

Use the `debug ip pimdm packet` command to trace PIMDM packet reception and transmission. The `receive` option traces only received PIMDM packets and the `transmit` option traces only transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.
Use the **no** form of this command to disable debug tracing of PIMDM packet reception and transmission.

### Syntax

```
debug ip pimdm packet [receive | transmit]
no debug ip pimdm packet [receive | transmit]
```

### Default Configuration

Display of PIMDM traces is disabled by default.

### Command Mode

Privileged Exec mode.

### User Guidelines

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

### Example

```
console#debug ip pimdm packet
```

### debug ip pimsm packet

Use the `debug ip pimsm` command to trace PIMSM packet reception and transmission. The **receive** option traces only received PIMSM packets and the **transmit** option traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the **no** form of this command to disable debug tracing of PIMSM packet reception and transmission.

### Syntax

```
debug ip pimsm packet [receive | transmit]
no debug ip pimsm packet [receive | transmit]
```
Default Configuration
Display of PIMSM traces is disabled by default.

Command Mode
Privileged Exec mode.

User Guidelines
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

Example
console#debug ip pimsm packet

debg ipv6 dhcp
Use the debug ipv6 dhcp command to display debug information about DHCPv6 client activities and to trace DHCPv6 packets to and from the local DHCPv6 client. To disable debugging, use the no form of the command.

Syntax
debg ipv6 dhcp
no debug ipv6 dhcp

Default Configuration
Debugging for the DHCP for IPv6 is disabled by default.

Command Mode
Privileged Exec

User Guidelines
This command enabled DHCPv6 packet tracing.
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.
Examples

```
console#debug ipv6 dhcp
```

depend ipv6 mcache

Use the `debug ipv6 mcache` command to trace MDATAv6 packet reception and transmission. The `receive` option traces only received data packets and the `transmit` option traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

**Syntax**

```
debug ipv6 mcache packet [receive | transmit]
no debug ipv6 mcache packet [receive | transmit]
```

**Default Configuration**

Display of MDATA traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
console#debug ipv6 mcache packet
```

depend ipv6 mld

Use the `debug ipv6 mld` command to trace MLD packet reception and transmission. The `receive` option traces only received MLD packets and the `transmit` option traces only transmitted MLD packets. When neither keyword is used in the command, then all MLD packet traces are dumped. Vital
information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable MLD tracing.

Syntax

debug ipv6 mld packet [receive | transmit]
no debug ipv6 mld packet [receive | transmit]

Default Configuration
Display of MLD traces is disabled by default.

Command Mode
Privileged Exec mode.

User Guidelines
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

Example
console#debug ipv6 mld packet

**debug ipv6 pimdm**

Use the debug ipv6 pimdm command to trace PIMDMv6 packet reception and transmission. The receive option traces only received PIMDMv6 packets and the transmit option traces only transmitted PIMDMv6 packets. When neither keyword is used in the command, then all PIMDMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMDMv6 tracing.

Syntax

debug ipv6 pimdm packet [receive | transmit]
no debug ipv6 pimd packet [receive | transmit]

**Default Configuration**
Display of PIMDMv6 traces is disabled by default.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**
```
console#debug ipv6 pimd packet
```

**debug ipv6 pimsm**
Use the `debug ipv6 pimsm` command to trace PIMSMv6 packet reception and transmission. The `receive` option traces only received PIMSMv6 packets and the `transmit` option traces only transmitted PIMSMv6 packets. When neither keyword is used in the command, then all PIMSMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMSMv6 tracing.

**Syntax**
```
depbug ipv6 pimsm packet [receive | transmit]
no debug ipv6 pimsm packet [receive | transmit]
```

**Default Configuration**
Display of PIMSMv6 traces is disabled by default.

**Command Mode**
Privileged Exec mode.
**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

console#debug ipv6 pimsm packet

**debug isdp**

Use the `debug isdp` command to trace ISDP packet reception and transmission. The `receive` option traces only received ISDP packets and the `transmit` option traces only transmitted ISDP packets. When neither keyword is used in the command, then all ISDP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable ISDP tracing.

**Syntax**

```
debug isdp packet [receive | transmit]
no debug isdp packet [receive | transmit]
```

**Default Configuration**

Display of ISDP traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

console#debug isdp packet
debug lACP

Use the `debug lACP` command to enable tracing of LACP packets received and transmitted by the switch. Use the “no” form of this command to disable tracing of LACP packets.

**Syntax**

d debug lACP packet
no debug lACP packet

**Default Configuration**

Display of LACP traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

c console#debug lACP packet

d debug mLDsnooping

Use the `debug mLDsnooping` command to trace MLD snooping packet reception and transmission. The receive option traces only received MLD snooping packets and the transmit option traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable tracing of MLD Snooping packets.
**Syntax**

debug mldsnooping packet [receive | transmit]

no debug mldsnooping packet [receive | transmit]

**Default Configuration**

Display of MLD Snooping traces is disabled by default.

**Command Mode**

Privileged Exec mode.

**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

console#debug mldsnooping

**debug ospf**

Use the `debug ospf` command to enable tracing of OSPF packets received and transmitted by the switch. Use the `no` form of this command to disable tracing of OSPF packets.

Use of the optional VRF parameter executes the command within the context of the VRF specific routing table.

**Syntax**

debug ospf packet [vrf vrf-name]

no debug ospf packet

- **vrf-name**—The name of the VRF associated with the routing table context used by the command. If no vrf is specified, the global routing table context is used.

**Default Configuration**

Display of OSPF traces is disabled by default.
Command Mode
Privileged Exec mode.

User Guidelines
The VRF identified in the parameter must have been previously created or an error is returned.
Only IPv4 addresses are supported with the `vrf` parameter.
This command is only available on the N3000/N3100/N4000 switches.
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

Example
console#debug ospf packet

debug ospfv3
Use the `debug ospfv3` command to enable tracing of OSPFv3 packets received and transmitted by the switch. Use the “no” form of this command to disable tracing of OSPFv3 packets.

Syntax
debug ospfv3 packet
no debug ospfv3 packet

Default Configuration
Display of OSPFv3 traces is disabled by default.

Command Mode
Privileged Exec mode.

User Guidelines
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.
debug ping

Use the debug ping command to enable tracing of ICMP echo requests and responses. This command traces pings on the network port and on the routing interfaces. Use the no form of this command to disable tracing of ICMP echo requests and responses.

Use of the optional vrf parameter executes the command within the context of the VRF specific routing table.

Syntax

d debug ping packet [vrf vrf-name]
no debug ping packet

• vrf-name—The name of the VRF associated with the routing table context used by the command. If no vrf is specified, the global routing table context is used.

Default Configuration

Display of ICMP echo traces is disabled by default.

Command Mode

Privileged Exec mode.

User Guidelines

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the vrf parameter.

This command is only available on the N3000/N3100/N4000 switches.

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.
Example
The following example displays.

```
console#debug ping packet
```

**debug rip**
Use the `debug rip` command to enable tracing of RIP requests and responses. Use the `no` form of this command to disable tracing of RIP requests and responses.

**Syntax**
```
debug rip packet
no debug rip packet
```

**Default Configuration**
Display of RIP traces is disabled by default.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

```
Example
console#debug rip packet
```

**debug sflow**
Use the `debug sflow` command to enable sFlow debug packet trace. Use the `no` form of this command to disable sFlow packet tracing.

**Syntax**
```
debug sflow packet
no debug sflow packet
```
**Default Configuration**
Display of sFlow traces is disabled by default.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

```
core#debug sflow packet
```

**debug spanning-tree**
Use the `debug spanning-tree` command to trace spanning tree BPDU packet reception and transmission. The `receive` option traces only received spanning tree BPDUs and the `transmit` option traces only transmitted BPDUs. When neither keyword is used in the command, all spanning tree BPDU traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the `no` form of this command to disable tracing of spanning tree BPDUs.

**Syntax**
```
debug spanning-tree bpdu [receive | transmit]
no debug spanning-tree bpdu [receive | transmit]
```

**Default Configuration**
Display of spanning tree BPDU traces is disabled by default.

**Command Mode**
Privileged Exec mode.
**User Guidelines**

Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**Example**

console#debug spanning-tree bpdu

**debug udld**

Use the `debug udld` command to enable the display of UDLD packets or event processing.

Use the `no` form of the command to disable debugging.

**Syntax**

```
debug udld {packet [receive | transmit] | events}
no debug udld {packet [receive | transmit] | events}
```

- **Packet**—Display transmitted and received UDLD packets.
- **Receive**—Debug packets received by the switch.
- **Transmit**—Debug packets transmitted by the switch.
- **Events**—Display UDLD events.

**Default Configuration**

By default, debugging is disabled.

**Command Mode**

Privileged Exec mode

**User Guidelines**

Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.
**debug vpc**

Use the `debug vpc` command to enable debug traces for the specified protocols. Use the no form of the command to disable all or some of the debug trace display.

**Syntax**

ddebug vpc {peer-keepalive [packet] | peer-link {control-message | data-message} | peer detection | core}

no debug vpc [{peer-keepalive [packet] | peer-link {control-message | data-message} | peer detection | core]

- **peer-keepalive**—Displays the debug traces for the keepalive state machine transitions. The packet option enables debug traces for the keepalive packets exchanged between the MLAG peer devices on the peer link.
- **peer-link**—In error cases, enables the debug traces for the control messages or data messages exchanged between the MLAG devices on the peer link.
- **peer detection**—Enables the debug traces dual control plane detection protocol. Traces are seen when DCPDP state changes occur (enable/disable, peer detected…).
- **core**—Displays the MLAG core messages.

**Default Configuration**

This command has no default configuration.

**Command Modes**

Global Configuration mode

**User Guidelines**

Debug commands should be used with caution. Switch behavior may be adversely affected by the additional processing load incurred by enabling debug output.

**Example**

```
console#debug vpc peer-link data-message
```
VPC peer link data message tracing enabled.

**debug vrrp**

Use the `debug vrrp` command to enable VRRP debug protocol messages. Use the `no` form of this command to disable VRRP debug protocol messages.

**Syntax**

debug vrrp all  
no debug vrrp all

**Default Configuration**
The display of VRRP traces is disabled by default.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
Debug output should be enabled with caution. Switch behavior may be adversely affected by the additional processing load incurred from enabling debug.

**exception core-file**

Use the `exception core-file` command to configure the core dump file name. Use the `no` form of the command the reset the core file name to the default.

**Syntax**

eception core-file file-name [hostname [time-stamp] | time-stamp [hostname]]  
no exception core-file

- file-name — The file name. The maximum length is 15 characters. Embedded blanks may not be allowed by the host file system (for example, TFTP server) and are not recommended.
Switch Management Commands

• **hostname** — Includes the switch host name in the core file name. If not configured, uses the switch MAC address in the core file name.
• **time-stamp** — Includes the switch TOD in the core file name.

**Default Configuration**

By default, the core file name has no prefix and no host name and uses the time stamp of the switch in the core file name.

**Command Modes**

Global Configuration mode

**User Guidelines**

The configuration parameters are not validated when this command is entered. Use the `write core test` command to validate the configured parameters and that the core dump is likely to succeed.

An average core file is around 450 KB. Example copy times are as follows:

- TFTP: 13mins (different subnet)
- USB: 3 mins

Administrators should ensure that a cleanly formatted USB flash drive of at least 1G is used for collection of a the full core dump. Do not remove the USB device during data transfer. Use the `unmount` command to cleanly detach the USB device prior to physical removal.

**Example**

This example enables core dumps to a TFTP server 10.27.9.1 reachable over the out-of-band port. The core file is written to the dumps directory and the name includes the host name of the switch and the switch TOD.

```
console(config)#exception dump tftp-server 10.27.9.1 file-path dumps
console(config)#exception core-file hostname time-stamp
console(config)#exception protocol tftp
```

**exception dump**

Use this command to configure the core dump location. Use the `no` form of the command to reset the location and parameters to the default values.
### Syntax

```
exception dump {tftp-server ip-address | ftp-server ip-address [username user-name {nopassword | password password}] | file-path dir | compression | stack-ip-address [protocol {dhcp | static} | add ip-address netmask [gateway]]}

no exception dump {tftp-server | file-path}
```

- **ip-address**—The IPv4 address of a TFTP server.
- **ftp-server**—Transfer the core information to an FTP server.
- **username**—The login id on the FTP server
- **nopassword**—The user id configured on the FTP server does not require a password.
- **password**—The user id configured on the FTP server requires a password.
- **file-path**—The directory to prepend to the core file name.
- **protocol dhcp**—Obtain the out-of-band port address via DHCP for core dump transfer.
- **protocol static**—Use a statically assigned address for core dump transfer

### Default Configuration

Debug core dumps are disabled by default.
The out-of-band port attempts to retrieve an IP address via DHCP by default.
No TFTP or FTP server is defined.
No stack IP addresses are assigned
Compression is enabled by default

### Command Modes

Global Configuration mode

### User Guidelines

This option should only be used under the direction of Dell support personnel.
The **file-path** parameter is used by both the USB and TFTP core dumps.
The TFTP or FTP server must be reachable over the out-of-band interface. Front panel ports cannot be used during exception processing.

Configuration parameters are not validated when the command is entered. Use the `write core test` command to validate the configured parameters and that the core dump is likely to succeed.

Crash dump retrieval via FTP or TFTP occurs after the system has crashed. During this time, the switch is not available for normal operation.

If no DHCP server is available for assignment of addresses to switches, the `exception dump stack-ip-address protocol static add` command should be used once for each member of the stack. It is recommended that these addresses be unique in the network. The stack master will distribute the addresses to the stack members for use on the out-of-band port only during crash dump transfer. In addition, for the purposes of transferring the core file to the server, a unique MAC address is assigned to the stack unit. As crash dump retrieval is not reliable on the front panel ports, the TFTP and FTP parameters are not available on the N1100-ON/N2100-ON/N1500/N2000 Series switches. Use the USB crash dump capability instead.

**Example**

This example enables core dumps to a TFTP server 10.27.9.1 reachable over the out-of-band port. The core file is written to the “dumps” directory and the name includes the host name of the switch and the switch TOD.

```
console(config)#exception dump tftp-server 10.27.9.1 file-path dumps
console(config)#exception core-file Core hostname time-stamp
console(config)#exception protocol tftp
```

**exception protocol**

Use the `exception protocol` command as directed by Dell EMC Networking support to enable full core dumps. Use the `no` form of the command to disable full core dumps.

**Syntax**

```
exception protocol {local | tftp | ftp | usb | none}
```

**no exception protocol**

- `local`—Save the core file on the local file system.
Switch Management Commands

- **tftp** — Store the core dump on a TFTP server reachable on the out-of-band port.
- **ftp** — Enable core transfer to an FTP server reachable on the out-of-band port.
  - user-name — The login id on the FTP server.
  - **nopassword** — The user id configured on the FTP server does not require a password.
  - **password** — The user id configured on the FTP server requires a password.
  - password — The password associated with the user id on the FTP server.
  - ip address — The IPv4 address of an FTP or TFTP server.
- **usb** — Store the core dump on a USB device. A USB device must be inserted into the switch front panel.
- **none** — Core dumps are disabled.

Stack-ip-address parameters:
- **ipv4-address** — The address used by the of the out-of-band port of the switch during crash dump transfer.
- netmask — The netmask for use with the ip address for core dump transfer.
- gateway — The default gateway to use on the out-of-band port for core dump transfer.
- **protocol dhcp** — Obtain the out-of-band port address via DHCP for core dump transfer.
- **protocol static** — Use a statically assigned address for core dump transfer.

**Default Configuration**
Debug core dumps are disabled by default.
The out-of-band port attempts to retrieve an IP address via DHCP by default.
No TFTP or FTP server is defined.
No stack IP addresses are assigned
Compression is enabled by default

**Command Modes**
Global Configuration mode
User Guidelines

Crash dump retrieval via FTP or TFTP occurs after the system has crashed. During this time, the switch is not available for normal operation.

If no DHCP server is available for assignment of addresses to switches, the `exception dump stack-ip-address protocol static add` command should be used once for each member of the stack. It is recommended that these addresses be unique in the network. The stack master will distribute the addresses to the stack members for use on the out-of-band port only during crash dump transfer. In addition, for the purposes of transferring the core file to the server, a unique MAC address is assigned to the stack unit.

As crash dump retrieval is not reliable on the front panel ports, the TFTP and FTP parameters are not available on the N1100-ON/N1500/N2000/N2100 series switches. Use the USB crash dump capability instead.

Example

This example enables core dumps to a TFTP server 10.27.9.1 reachable over the out-of-band port. The core file is written to the dumps directory and the name includes the host name of the switch and the switch TOD.

```
console(config)#exception dump tftp-server 10.27.9.1 file-path dumps
cfg exile(config)#exception core-file Core hostname time-stamp
console(config)#exception protocol tftp
```

This example enables core dumps to a USB flash drive. The core file is written to the top level directory and the name includes the host name of the switch and the switch TOD.

```
console(config)#exception core-file Core hostname time-stamp
console(config)#exception protocol usb
console(config)#do dir usb
```

```
Attr  Size(bytes)          Creation Time        Name
drwx  16384 Jan 01 1980 00:00:00 .
drwx                  0 Dec 16 2014 18:25:43 ..
-rwx                 943 Jan 01 1980 00:00:00 start.scr
-rwx            21642899 Jan 01 1980 00:00:00 backup.stk
-rwx                 373 Jan 01 1980 00:00:00 start.text
-rwx                 37549 Aug 21 2013 07:55:22 maxacl.scr
-rwx                33903 Aug 22 2013 10:49:38 max-acls-per-list.scr
-rwx                139874 Oct 09 2013 14:00:18 max-ipv4-acls.scr
-rwx                 5899 Sep 20 2013 14:23:26 local_repro.txt
-rwx             21262857 Oct 24 2013 12:12:30 N4000vD.10.23.2.stk
```

Total Size: 1002160128
exception switch-chip-register

Use the `exception switch-chip-register` command to enable dumping the switch chip registers in case of an exception. The register dump is taken only for the master unit and not for the stack member units. Use the `no` form of the command to disable dumping of the switch-chip registers.

**Syntax**

```
exception switch-chip-register
no exception switch-chip-register
```

**Default Configuration**

By default, switch register dumps are disabled.

**Command Modes**

Global Configuration mode

**User Guidelines**

This option should only be used under the direction of Dell support personnel.
Switch registers are captured to the local file system.

ip http timeout-policy

Use the `ip http timeout-policy` command to configure the timeout policy for closing HTTP and HTTPS sessions to the local HTTP server.

**Syntax**

```
ip http timeout-policy idle seconds life seconds
no ip http timeout-policy
```
• seconds—For the **idle** parameter, the approximate number of seconds after which an idle connection is closed. For the **life** parameter, the approximate number of seconds since login after which a session is closed.

**Default Configuration**

The default values are as follows:

- **idle**—180 seconds. Range: 1-3600
- **life**—1800 seconds. Range: 1-86400

**Command Mode**

Global Configuration

**User Guidelines**

This command configures the timeout for both HTTP and HTTPS sessions. Changes to the parameters affect existing sessions. Reducing the time parameters may close existing sessions.

The idle timeout closes sessions in which no activity is detected (e.g., no commands are entered). The life timeout specifies the maximum number of seconds a session will be kept open from the time the session was established. Times are approximate.

Use this command to establish an access policy which maximizes throughput or minimizes response time for new connections. For minimal response time for new connections, use smaller values. For maximizing throughput (e.g., with dedicated management connections), use larger values.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```bash
console(config)#ip http timeout-policy idle 3600 life 86400
```

**show debugging**

Use the `show debugging` command to display packet tracing configurations.


**Syntax**

show debugging

no show debugging

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Enabled packet tracing configurations are displayed.

**Example**

console#show debugging

Authentication manager all debug traces enabled on Gi1/0/1
show exception

Use the show exception command to display the core dump configuration parameters, the current or previous exception log, or the core dump file listing.

Syntax

show exception [log [previous] | core-dump-file]
  • log—Display the current exception log.
  • log previous—Display the previous exception log.
  • core-dump-file—Display the core-dump file listing.

Default Configuration

This command has no default configuration.

Command Modes

Privileged Exec mode (all show modes)

User Guidelines

An exception log or core dump file is generated in the rare event that the switch firmware fails. Dell support personnel may ask administrators to provide the exception log information to assist in issue resolution.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coredump file name</td>
<td>Core dump file name</td>
</tr>
<tr>
<td>Coredump filename uses hostname</td>
<td>Core file name includes host name (True or False)</td>
</tr>
<tr>
<td>Coredump filename uses time-stamp</td>
<td>Core file name users time stamp (True or False)</td>
</tr>
<tr>
<td>TFTP server IP</td>
<td>TFTP server IP address</td>
</tr>
<tr>
<td>FTP server IP</td>
<td>FTP server IP address</td>
</tr>
<tr>
<td>FTP user name</td>
<td>FTP server account user name</td>
</tr>
<tr>
<td>FTP password</td>
<td>FTP server account user password</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File path</td>
<td>File path for TFTP or FTP server</td>
</tr>
<tr>
<td>Protocol</td>
<td>Exception protocol (TFTP, USB, Core - default none).</td>
</tr>
<tr>
<td>Switch-chip-register</td>
<td>Include register dump (True or False)</td>
</tr>
<tr>
<td>Compression mode</td>
<td>Compress core file (True or False)</td>
</tr>
<tr>
<td>Stack IP Address Protocol</td>
<td>Obtain switch IP address (DHCP or Static)</td>
</tr>
</tbody>
</table>

**Example**

The following example shows the default core transfer values.

```console
console(config)#show exception
```

Coredump file name............................. crash
Coredump filename uses hostname.............. False
Coredump filename uses time-stamp.............. False
TFTP server IP.................................
FTP server IP..................................
FTP user name..................................
FTP password...................................
File path...................................... dumps
Protocol....................................... none
Switch-chip-register......................... False
Compression mode............................... TRUE
Stack IP Address Protocol...................... dhcp
Stack IP Address:
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Net Mask</th>
<th>Gateway</th>
<th>Assigned Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**show supported mibs**

Use the **show supported mibs** command to display the implemented SNMP MIBs.

**Syntax**

```
show supported mibs
```
**Default Configuration**
There is no default configuration for this command.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
There are no user guidelines for this command.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
```
console#show supported mibs
```

MIBs Supported:

- **RFC 1907 - SNMPv2-MIB**: The MIB module for SNMPv2 entities
- **RFC 2819 - RMON-MIB**: Remote Network Monitoring Management Information Base
- **HC-RMON-MIB**: The original version of this MIB, published as RFC3273.
- **HC-ALARM-MIB**: Initial version of the High Capacity Alarm MIB module. This version published as RFC 3434.
- **HCNUM-TC**: A MIB module containing textual conventions for high capacity data types.
- **DELL-REF-MIB**: DELL Reference
- **SNMP-COMMUNITY-MIB**: This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
- **SNMP-FRAMEWORK-MIB**: The SNMP Management Architecture MIB
- **SNMP-MPD-MIB**: The MIB for Message Processing and Dispatching
- **SNMP-NOTIFICATION-MIB**: The Notification MIB Module
- **SNMP-TARGET-MIB**: The Target MIB Module
- **SNMP-USER-BASED-SM-MIB**: The management information definitions for the SNMP User-based Security Model.
- **SNMP-VIEW-BASED-ACM-MIB**: The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB
DELL-POWER-ETHERNET-MIB
POWER-ETHERNET-MIB
SFLOW-MIB
DELL-SFLOW-MIB
DELL-ISDP-MIB
DELL-UDLD-MIB
DELL-BOXSERVICES-PRIVATE-MIB
DIFFSERV-DSCP-TC
IANA-ADDRESS-FAMILY-NUMBERS-MIB
DELL-DHCPSERVER-PRIVATE-MIB
DELL-DHCPCLIENT-PRIVATE-MIB
DELL-DNS-RESOLVER-CONTROL-MIB
DELL-DENIALOFSERVICE-PRIVATE-MIB
DELL-GREENETHERNET-PRIVATE-MIB
DELL-DEVICE-FILESYSTEM-MIB
DELL-KEYING-PRIVATE-MIB
LLDP-MIB
LLDP-EXT-DOT3-MIB
LLDP-EXT-MED-MIB
DELL-LLPF-PRIVATE-MIB
DISMAN-PING-MIB
DNS-SERVER-MIB

SNMP Research, Inc.
DELL Power Ethernet Extensions MIB
Power Ethernet MIB
sFlow MIB
The DELL Private MIB for DELL SFlow
Industry Standard Discovery Protocol MIB
UDLD MIB
The DELL Private MIB for DELL Box Services Feature.
The Textual Conventions defined in this module should be used whenever a Differentiated Services Code Point is used in a MIB.
The MIB module defines the AddressFamilyNumbers textual convention.
The DELL Private MIB for DELL DHCP Server
The DELL Private MIB for DELL DHCP Client
Defines a portion of the SNMP MIB under the DELL Corporation enterprise OID pertaining to DNS Client control configuration
The DELL Private MIB for DELL Denial of Service.
The MIB definitions for DELL Green Ethernet
The DELL Private MIB for DELL DeviceFileSystem
The DELL Private MIB for DELL Keying Utility
Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
The LLDP Management Information Base extension module for IEEE 802.3 organizationally defined discovery information.
The LLDP Management Information Base extension module for TIA-TR41.4 Media Endpoint Discovery information.
The DELL Private MIB for DELL Link Local Protocol Filtering.
The Ping MIB (DISMAN-PING-MIB) provides the capability of controlling the use of the ping function at a remote host.
The MIB module for entities implementing the server side of the Domain Name System (DNS) protocol.

Switch Management Commands
DNS-RESOLVER-MIB

The MIB module for entities implementing the client (resolver) side of the Domain Name System (DNS) protocol.

SMON-MIB

The MIB module for managing remote monitoring device implementations for Switched Networks.

DELL-OUTBOUNDTELNET-PRIVATE-MIB

The DELL Private MIB for DELL Outbound Telnet

DELL-TIMERANGE-MIB

The DELL Private MIB for DELL Time Ranges

DELL-TIMEZONE-PRIVATE-MIB

The DELL Private MIB for DELL system time, timezone and summer-time settings

DISMAN-TRACEROUTE-MIB

The Traceroute MIB (DISMAN-TRACEROUTE-MIB) provides access to the traceroute capability at a remote host.

LAG-MIB

The Link Aggregation module for managing IEEE 802.3ad

RFC 1213 - RFC1213-MIB

Management Information Base for Network Management of TCP/IP-based internets: MIB-II

RFC 1493 - BRIDGE-MIB

Definitions of Managed Objects for Bridges (dot1d)

RFC 2674 - P-BRIDGE-MIB

The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.

RFC 2674 - Q-BRIDGE-MIB

The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks

RFC 2737 - ENTITY-MIB

Entity MIB (Version 2)

RFC 2863 - IF-MIB

The Interfaces Group MIB using SMIv2

RFC 3635 - Etherlike-MIB

Definitions of Managed Objects for the Ethernet-like Interface Types

DELL-SWITCHING-MIB

DELL Switching - Layer 2

DELL-INVENTORY-MIB

Unit and Slot configuration.

DELL-PORTSECURITY-PRIVATE-MIB

Port Security MIB.

INET-ADDRESS-MIB

This MIB module defines textual conventions for representing Internet addresses.

IANAifType-MIB

This MIB module defines the IANAifType Textual Convention

DELL-LOGGING-MIB

This MIB provides objects to configure and display events logged on this system.

MAU-MIB

Management information for 802.3 MAUs.

DELL-MVR-PRIVATE-MIB

The DELL Private MIB for MVR Configuration

DELL-SNTP-CLIENT-MIB

Defines DELL Corporation enterprise OID pertaining to SNTP client configuration and statistical collection.

DELL-VFC-MIB

The MIB definitions for VFC.

IEEE8021-PAE-MIB

Port Access Entity module for managing IEEE 802.1X.
DELL-DOT1X-ADVANCED-FEATURES-MIB
The DELL Private MIB for DELL Dot1x Advanced

DELL-DOT1X-AUTHENTICATION-SERVER-MIB
The DELL Private MIB for DELL Dot1x Authentication Server

DELL-RADIUS-AUTH-CLIENT-MIB
The DELL Private MIB for DELL RADIUS Authentication Client.

RADIUS-ACC-CLIENT-MIB
RADIUS Accounting Client MIB

RADIUS-AUTH-CLIENT-MIB
RADIUS Authentication Client MIB

TACACS-CLIENT-MIB
Defines a portion of the SNMP MIB under the DELL Corporation enterprise OID pertaining to TACACS+ client configuration.

DELL-CAPTIVE-PORTAL-MIB
DELL Captive Portal MIB

DELL-AUTHENTICATION-MANAGER-MIB
The DELL Private MIB for DELL authentication manager feature.

DELL-MGMT-SECURITY-MIB
The DELL Private MIB for DELL Mgmt Security

RFC 1724 - RIPv2-MIB
RIP Version 2 MIB Extension

RFC 1850 - OSPF-MIB
OSPF Version 2 Management Information Base

RFC 1850 - OSPF-TRAP-MIB
The MIB module to describe traps for the OSPF Version 2 Protocol.

RFC 2787 - VRRP-MIB
Definitions of Managed Objects for the Virtual Router Redundancy Protocol

DELL-ROUTING-MIB
DELL Routing - Layer 3

IP-FORWARD-MIB
The MIB module for the management of CIDR multipath IP Routes.

IP-MIB
The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes.

DELL-LOOPBACK-MIB
The DELL Private MIB for DELL Loopback

RFC 1657 - BGP4-MIB
Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIV2

DELL-BGP-MIB
The MIB definitions for Border Gateway Protocol Flex package.

DELL-QOS-MIB
DELL Flex QOS Support

DELL-QOS-ACL-MIB
DELL Flex QOS ACL

DELL-QOS-COS-MIB
DELL Flex QOS COS

DELL-QOS-AUTOVOIP-MIB
DELL Flex QOS VOIP

DELL-QOS-DIFFSERV-PRIVATE-MIB
DELL Flex QOS DiffServ Private MIBs' definitions

DELL-QOS-ISCSI-MIB
DELL Flex QOS iSCSI Flow Acceleration MIBs' definitions

RFC 2932 - IPMROUTE-MIB
IPv4 Multicast Routing MIB

draft-ietf-magma-mgmd-mib-03
MGMD MIB, includes IGMPv3 and MLDv2.

RFC 5060 - PIM-STD-MIB
Protocol Independent Multicast MIB

RFC 5240 - PIM-BSR-MIB
Bootstrap Router mechanism for PIM routers
DVMRP-STD-MIB                      Distance-Vector Multicast Routing Protocol MIB
IANA-RTPROTO-MIB                   IANA IP Route Protocol and IP MRoute Protocol Textual Conventions
DELL-MULTICAST-MIB                 The MIB definitions for Multicast Routing Flex package.
IPMROUTE-STD-MIB                   The MIB module for management of IP Multicast routing, but independent of the specific multicast routing protocol in use.
MGMD-STD-MIB                       The MIB module for MGMD Management.
DELL-NSF-MIB                       The MIB module defines objects to configure Non Stop Forwarding.
RFC 2465 - IPV6-MIB                Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 - IPV6-ICMP-MIB          Management Information Base for IP Version 6: ICMPv6 Group
RFC 3419 - TRANSPORT-ADDRESS-MIB  Textual Conventions for Transport Addresses
DELL-ROMING6-MIB                   The DELL Private MIB for DELL IPv6 Routing.
DELL-DHCP6SERVER-PRIVATE-MIB      The DELL Private MIB for DELL DHCPv6 Server/Relay
DELL-IPV6-LOOPBACK-MIB            The DELL Private MIB for DELL Loopback IPv6 address configuration.
DELL-IPV6-TUNNEL-MIB              The DELL Private MIB for DELL IPv6 Tunnel.
Dell-LAN-SYSMNG-MIB                Management functions applicable to all Dell Networking managed switches
Dell-LAN-TRAP-MIB                  Dell alarms specific global parameters
Dell-Vendor-MIB                    This MIB allows Dell Networking devices to be integrated into Dell ITA management system.

**snapshot bgp**

Use the **snapshot bgp** command in support mode to dump the current state of BGP for use by support personnel.

**Syntax**

**snapshot bgp**
Default Configuration
There is no default configuration.

Command Mode
Support mode

User Guidelines
This command has no user guidelines.

Command History
Introduced in version 6.2.0.1 firmware.

write core
Use the write core command to generate a core file on demand and either reboot the switch or test the core file configuration.

Syntax
write core [test [dest-file-name]]
  •  dest-file-name — The file name used if a tftp-server is configured with the exception dump tftp-server command. The dest-file-name parameter overrides the file name parameters configured with the exception core-file command.

Default Configuration
This command has no default configuration.

Command Modes
Privileged Exec mode

User Guidelines
Using the write core command reboots the switch. The write core command is useful when the device malfunctions, but has not crashed.
The **write core test** command is useful for validating the core dump setup. For example, if the protocol is configured as tftp, the command write core test communicates with the tftp server and informs the administrator if the tftp server can be contacted. Similarly, if the protocol is configured as usb, it mounts and unmounts the file system and then informs the administrator regarding the status.

**Example**

```
console#write core
The system has unsaved changes.
Would you like to save them now? (y/n) n
Configuration Not Saved!
This operation will reboot the device.
Are you sure you want to create coredump? (y/n).y
----------------------------------------------------
Thu Jan 1 00:17:35 1970
[pgid:577] [pid:577] [name:(syncdb)] [signal:11]
Call Trace (depth = 3):
  0xb6faf7dc
  0xb6fafc60
  0xb6ef742c
<188> Jan 1 00:17:36 10.27.22.174-1 General[80499188]: procmgr.c(2926) 1171
  %% Application Terminated (syncdb, ID = 2, PID = 577
  log_error_code osapi_crash.c 2010

Switching software SIGSEGV Handler
This build was configured to copy this crash information to a file.
```
Sflow Commands

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a stand-alone probe) and a central sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow datagrams are used to forward the sampled traffic statistics immediately to an sFlow Collector for analysis. The traffic samples sent to the Collector contain the source ifIndex and, for switched packets, the destination ifIndex.

The sFlow Agent supports two forms of sampling: statistical packet-based sampling of switched or routed Packet Flows and time-based sampling of counters.

Commands in this Section

This section explains the following commands:

- `sflow destination`  
- `sflow polling`  
- `sflow polling (Interface Mode)`  
- `sflow sampling`  
- `sflow sampling (Interface Mode)`  
- `sflow source-interface`  
- `show sflow agent`  
- `show sflow destination`  
- `show sflow polling`  
- `show sflow sampling`  
- `show sflow source-interface`  
- `-`  

sflow destination

Use the `sflow destination` command to configure the sFlow collector parameters (owner string, receiver timeout, maxdatagram, ip address and port). Use the “no” form of this command to set receiver parameters to the default or remove a receiver.
**Syntax**

```
sflow rcvr_index destination {ip-address [port] | maxdatagram size | owner “owner_string” {notimeout | timeout rcvr_timeout}}
```

```
no sflow rcvr_index destination [ip-address | maxdatagram | owner]
```

- **rcvr_index** — The index of this sFlow Receiver (Range: 1–8).
- **ip-address** — The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent.
- **size** — The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. (Range: 200–9116 bytes).
- **owner_string** — The identity string for the receiver. A receiver is not enabled until the owner string is assigned. The default is an empty string. The identity string must be set before assigning a receiver to a sampler or poller. (Range: 1–127 characters).
- **rcvr_timeout** — The time, in seconds, remaining before the sampler or poller is released and stops sending samples to the receiver. Setting a value of 0 for the timeout value permanently configures the sflow receiver. Use the no form of the command to remove permanently configured receivers. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. (Range: 0–2147483647 seconds).
- **port** — The destination Layer4 UDP port for sFlow datagrams. (Range: 1–65535).

**Default Configuration**

No receivers are configured by default.
The default IP address is 0.0.0.0
The default maximum datagram size is 1400.
The default owner string is the empty string.
The default receiver timeout is 0.
The default destination port is 6343.

**Command Mode**

Global Configuration mode.
User Guidelines

An sflow destination entry must have an owner assigned in order for polling or sampling to be operational. The last set of command parameters are optional in the no form of the command. Sflow commands with a timeout value supplied do not show in the running config. Because the timer is actively running, the command is ephemeral and is therefore not shown in the running config. Entering an sflow command with a notimeout parameter will cause the sflow configuration to be shown in the running config.

Example

```
console(config)#sflow 1 destination owner 1 timeout 2000
console(config)#sflow 1 destination maxdatagram 500
console(config)#sflow 1 destination 30.30.30.1 560
```

sflow polling

Use the sflow polling command to enable a new sflow poller instance for this data source if rcvr_idx is valid. An sflow poller sends counter samples to the receiver. Use the “no” form of this command to reset poller parameters to the defaults.

Syntax

```
sflow rcvr-index polling {gigabitethernet | tengigabitethernet | fortygigabitethernet} interface-list poll-interval

no sflow rcvr-index polling {gigabitethernet | tengigabitethernet | fortygigabitethernet} interfaces
```

- rcvr-index — The sFlow Receiver associated with the poller (Range: 1–8).
- interface-list — The list of interfaces to poll in unit/slot/port format.
- poll-interval — The sFlow instance polling interval. A poll interval of 0 disables counter sampling. A value of n means once in n seconds a counter sample is generated. (Range: 0–86400).

Default Configuration

There are no pollers configured by default.

The default poll interval is 0.
**Command Mode**
Global Configuration mode.

**User Guidelines**
The sflow instance must be configured using the `sflow destination owner` command before this command can successfully execute.

**Example**
```
console(config)#sflow 1 polling gigabitethernet 1/0/1-10 200
```

**sflow polling (Interface Mode)**
Use the `sflow polling` command in Interface Mode to enable a new sflow poller instance for this interface if `rcvr_idx` is valid. An sflow poller sends counter samples to the receiver. Use the `no` form of this command to reset poller parameters to the defaults.

**Syntax**
```
sflow rcvr-index polling poll-interval
no sflow rcvr-index polling
```
- `rcvr-index` — The sFlow Receiver associated with the poller (Range: 1 - 8).
- `poll-interval` — The sFlow instance polling interval. A poll interval of 0 disables counter sampling. A value of n means once in n seconds a counter sample is generated. (Range: 0 - 86400).

**Default Configuration**
There are no pollers configured by default.
The default poll interval is 0.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**
This command has no user guidelines.
Example
console(config-if-Gi1/0/2)#sflow 1 polling 6055

sflow sampling
Use the sflow sampling command to enable a new sFlow sampler instance for this data source if rcvr_idx is valid. An sFlow sampler collects flow samples to send to the receiver. Use the “no” form of this command to reset sampler parameters to the default.

Syntax
sflow rcvr-index sampling {gigabitethernet | tengigabitethernet | fortygigabitethernet} interface-list sampling-rate [size]
no sflow rcvr-index sampling {gigabitethernet | tengigabitethernet | fortygigabitethernet} interface-list

- rcvr-index—The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. If no receiver is configured, then no packets will be sampled. Only active receivers can be set. If a receiver times out, then all samplers associated with the receiver will also expire. (Range: 1–8).
- interface-list — The list of interfaces to poll in unit/slot/port format.
- sampling-rate—The statistical sampling rate for packet sampling from this source. A value of n means that out of n incoming packets, 1 packet will be sampled. (Range: 1024–65536).
- size—The maximum number of bytes that should be copied from the sampler packet (Range: 20–256 bytes).

Default Configuration
There are no samplers configured by default.
The default is no default sampling rate.
The default size is 128.

Command Mode
Global Configuration mode.
User Guidelines

Lower sampling numbers cause more samples to be collected and increase the load on the CPU. Setting a sampling rate of 1024 on a large number of ports may tax the CPU beyond its ability to deliver the packets to the receiver. Lowering the sampling rate (higher numerical value) will help to ensure that all collected samples can be sent to the receiver. The sflow instance must be configured using the sflow destination owner command before this command can successfully execute.

Example

console(config)#sflow 1 sampling gigabitethernet 1/0/2 1500 50

sflow sampling (Interface Mode)

Use the sflow sampling command in Interface Mode to enable a new sflow sampler instance for this data source if rcvr_idx is valid. Use the no form of this command to reset sampler parameters to the default.

Syntax

sflow rcvr-index sampling sampling-rate [size]
no sflow rcvr-index sampling

- rcvr-index — The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. If no receiver is configured, then no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. (Range: 1 - 8).
- sampling-rate — The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A rate of 0 disables sampling. A value of n means that out of n incoming packets, 1 packet will be sampled. (Range: 1024 - 65536).
- size — The maximum number of bytes that should be copied from the sampler packet (Range: 20 - 256 bytes).

Default Configuration

There are no samplers configured by default.
There is no default sampling rate.
The default maximum header size is 128.
**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

Lower sampling numbers cause more samples to be collected and increase the load on the CPU. Setting a sampling rate of 1024 on a large number of ports may tax the CPU beyond its ability to deliver the packets to the receiver. Lowering the sampling rate (higher numerical value) will help to ensure that all collected samples can be sent to the receiver.

**Example**

```
console(config-if-Gi1/0/15)#sflow 1 sampling 1500 50
```

**sflow source-interface**

Use the `sflow source-interface` command to select the interface from which to use the IP address inserted in the source IP address field of transmitted sFlow packets. Use the no form of the command to revert to the default IP address.

**Syntax**

```
sflow source-interface {loopback loopback-id | vlan vlan-id | out-of-band | tunnel tunnel-id}
```

**no sflow source-interface**

- `loopback-id` — A loopback interface identifier.
- `vlan-id` — A VLAN identifier.
- `tunnel-id` — A tunnel identifier (Range 0–7).

**Default Configuration**

By default, the switch uses the assigned switch IP address as the source IP address for sFlow packets. This is either the IP address assigned to the VLAN from which the sFlow packet originates or the out-of-band interface IP address.
**Command Mode**
Global Configuration mode

**User Guidelines**
The source interface must have an assigned IP address (either manually or via another method such as DHCP). Use the `show sflow source-interface` command to display the assigned source interface. This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

The out-of-band parameter is only available on switches so equipped.

**Example**
```
console#conf
cconsole(config)#interface vlan 1
cconsole(config-if-vlan1)#ip address dhcp
cconsole(config-if-vlan1)#exit
cconsole(config)#sflow source-interface vlan 1
```

**show sflow agent**
Use the `show sflow agent` command to display the sflow agent information.

**Syntax**
```
show sflow agent
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following fields are displayed:
Example

console#show sflow agent

sFlow Version.......................... 1.3;Dell Inc.;10.23.18.28
IP Address............................. 10.27.21.34

show sflow destination

Use the show sflow destination command to display all the configuration information related to the sFlow receivers.

Syntax

show sflow rcvr-index destination
  • rcvr index—The index of the sFlow Receiver to display (Range: 1–8).

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The following fields are displayed:

| Receiver Index | The sFlow Receiver associated with the sampler/poller. |
Switch Management Commands

| Owner String | The identity string for receiver, the entity making use of this sFlowRcvrTable entry. |
| Time Out | The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. |
| IP Address | The destination IP address (the sFlow receiver host). |
| Address Type | 1 for IPv4 and 2 for IPv6. |
| Port | The destination Layer4 UDP port for sFlow datagrams. |
| Datagram Version | The sFlow record format version. For example, 5 indicates sFlow version 5. |
| Maximum Datagram Size | The maximum number of bytes that can be sent in a single sFlow datagram. |

**Example**

console(config)#show sflow 1 destination

Receiver Index................................. 1
Owner String................................... asd
Time out....................................... No Timeout
IP Address:.................................... 1.2.3.4
Address Type................................... 1
Port........................................... 6343
Datagram Version............................... 5
Maximum Datagram Size.......................... 1400

**show sflow polling**

Use the `show sflow polling` command to display the sFlow polling instances created on the switch.

**Syntax**

show sflow rcvr-index polling [{gigabitethernet | tengigabitethernet | fortygigabitethernet} interface-list]

- rcvr-index — The sFlow Receiver associated with the poller (Range: 1–8).
- interface-list — The list of interfaces to poll, in unit/slot/port format.
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
The following fields are displayed:

<table>
<thead>
<tr>
<th>Poller Data Source</th>
<th>The sFlowDataSource (unit/slot/port) for this sFlow sampler. This agent will support Ethernet ports only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Index</td>
<td>The sFlowReceiver associated with this sFlow counter poller.</td>
</tr>
<tr>
<td>Poller Interval</td>
<td>The number of seconds between successive samples of the counters associated with this data source.</td>
</tr>
</tbody>
</table>

Example
console# show sflow 1 polling

<table>
<thead>
<tr>
<th>Poller Data Source</th>
<th>Receiver</th>
<th>Poller Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel/0/1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

show sflow sampling

Use the `show sflow sampling` command to display the sFlow sampling instances created on the switch.

Syntax

```
show sflow rcvr-index sampling [{gigabitethernet | tengigabitethernet | fortygigabitethernet} interface-list]
```

- `rcvr-index` — The sFlow Receiver associated with the poller (Range: 1–8).
- `interface-list` — The list of interfaces on which data is sampled.
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The following fields are displayed:

<table>
<thead>
<tr>
<th>Sampler Data Source</th>
<th>The sFlowDataSource (unit/slot/port) for this sFlow sampler. This agent will support Ethernet ports only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Index</td>
<td>The sFlowReceiver configured for this sFlow sampler.</td>
</tr>
<tr>
<td>Packet Sampling Rate</td>
<td>The statistical sampling rate for packet sampling from this source.</td>
</tr>
<tr>
<td>Max Header Size</td>
<td>The maximum number of bytes that should be copied from a sampled packet to form a flow sample.</td>
</tr>
</tbody>
</table>

**Example**
```
console# #show sflow 1 sampling
```

```
Sampler Data Source | Receiver Index | Packet Sampling Rate | Max Header Size |
---------------------|-----------------|----------------------|-----------------|
Gi1/0/1 | 1 | 0 | 128 |
```

**show sflow source-interface**
Use the `show sflow source-interface` command to display the assigned sFlow source interface.

**Syntax**
```
show sflow source-interface
```

**Default Configuration**
This command has no defaults.
**Command Mode**
Privileged Exec, Global Configuration, and all sub-modes

**User Guidelines**
Use the `sflow source-interface` command to assign an IP address other than the default for transmitted sFlow packets. This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

**Example**
```
console#conf
console(config)#interface out-of-band
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#sflow source-interface out-of-band
console(config)#show sflow source-interface

sFlow Client Source Interface................. out-of-band
sFlow Client Source IPv4 Address............. 10.27.21.143          [Up]
sFlow Client Source IPv6 Address............. fe80::fab1:56ff:fe2b:a4fb   [Up]
```
SNMP Commands

The SNMP component provides a machine-to-machine interface for the Dell EMC Networking product family. This includes the ability to configure the network device, view settings and statistics, and upload or download code or configuration images. The agent includes a get-bulk command to reduce network management traffic when retrieving a sequence of Management Information Base (MIB) variables and an elaborate set of error codes for improved reporting to the network control station. The extensible and advanced design of the Dell EMC Networking SNMP makes adding remote manageability to networked devices undemanding. The agent allows a network control station to retrieve reports from the networked device. These reports are based upon the defined objects in the MIB. The agent queries, reports, and sets MIB variables based upon directions from the network control station or upon preset conditions.

Dell EMC Networking supports IPv4 and IPv6 SNMP access. Management access may be restricted to individual IPv4 and IPv6 management stations for management access and traps/informs. Management access may also be restricted to an IPv4 or IPv6 subnet.

Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>show snmp</th>
<th>snmp-server community</th>
<th>snmp-server group</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp engineid</td>
<td>snmp-server community-group</td>
<td>snmp-server host</td>
</tr>
<tr>
<td>show snmp filters</td>
<td>snmp-server contact</td>
<td>snmp-server location</td>
</tr>
<tr>
<td>show snmp group</td>
<td>snmp-server enable traps</td>
<td>snmp-server user</td>
</tr>
<tr>
<td>show snmp user</td>
<td>snmp-server engineID local</td>
<td>snmp-server view</td>
</tr>
<tr>
<td>show snmp views</td>
<td>snmp-server filter</td>
<td>snmp-server v3-host</td>
</tr>
<tr>
<td>show trapflags</td>
<td></td>
<td>snmp-server source-interface</td>
</tr>
</tbody>
</table>
**show snmp**

Use the `show snmp` command to display the SNMP communications status.

**Syntax**

`show snmp`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the SNMP communications status.

```
console(config)#show snmp

Community-String     Community-Access View Name     IP Address     IP Mask
-------------------- ------------------------------- ----------- -----------
private              Read/Write       Default          All             All
public               Read Only        Default          1.1.1.1 255.255.255.254

Community-String     Group Name       IP Address     IP Mask
-------------------- --------------------------- ---------- -----------
private              DefaultWrite     All             All
public               DefaultRead      All             All

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications
Target Address   Type  Community       Version UDP Filter  TO
Retries
```
show snmp engineid

Use the show snmp engineid command to display the ID of the local Simple Network Management Protocol (SNMP) engine.

**Syntax**

show snmp engineid

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The SNMP engine ID uniquely identifies the SNMP agent to other SNMPv3 stations. The SNMP engine ID is not cleared by the clear config command. The SNMP engine ID must be unique for the administrative domain.

**Example**

The following example displays the SNMP engine ID.
show snmp filters

Use the show snmp filters command to display the configuration of filters.

Syntax
show snmp filters filtername
- filtername — Specifies the name of the filter. (Range: 1-30)

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
Per RFC 2573, an implicit exclude all filter is present at the beginning of every filter list. This implicit filter is not shown in the output of this command.

Example
The following examples display the configuration of filters with and without a filter name specification.

```
console # show snmp filters
Name            OID Tree            Type
--------------- --------------------------
user-filter1    1.3.6.1.2.1.1            Included
user-filter1    1.3.6.1.2.1.1.7          Excluded
user-filter2    1.3.6.1.2.1.2.2.1.*.1    Included

console # show snmp filters user-filter1
Name            OID Tree            Type
--------------- --------------------------
user-filter1    1.3.6.1.2.1.1            Included
user-filter1    1.3.6.1.2.1.1.7          Excluded
```
show snmp group

Use the `show snmp group` command to display the configuration of groups.

Syntax

```plaintext
show snmp group [groupname]
```

- `groupname` — Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The group name accepts any printable characters except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

The following table contains field descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group</td>
</tr>
<tr>
<td>Security Model</td>
<td>SNMP model in use (v1, v2 or v3)</td>
</tr>
<tr>
<td>Security Level</td>
<td>Authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.</td>
</tr>
</tbody>
</table>
### Example

The following examples display the configuration of views.

```console
console# show snmp group

<table>
<thead>
<tr>
<th>Name</th>
<th>Security</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model  Level</td>
<td>Read  Write</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>user-group</td>
<td>V3 Auth-Priv</td>
<td>Default</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3 NoAuth-priv</td>
<td>Default</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3 NoAuth-priv</td>
<td>Default</td>
</tr>
</tbody>
</table>

```

```console
console#show snmp group DefaultWrite

<table>
<thead>
<tr>
<th>Name</th>
<th>Context</th>
<th>Security</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prefix</td>
<td>Model   Level</td>
<td>Read  Write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V1 NoAuth-NoPriv</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V2 NoAuth-NoPriv</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V3 NoAuth-NoPriv</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V3 Auth-NoPriv</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V3 Auth-Priv</td>
<td>Default</td>
</tr>
</tbody>
</table>

Command History

The example was updated in release 6.4.

### show snmp user

Use the `show snmp user` command to display the configuration of users.
### Syntax

show snmp user [username]

- **username** — Specifies the name of the user. (Range: 1-30)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

### User Guidelines

The user name accepts any printable characters except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

### Example

The following example displays the configuration of users with the user name specified.

```console
Console # show snmp user
Name          Group Name    Auth Meth     Priv Meth   Remote Engine ID
--------------- --------------- ---- ---- -------------------
bob               user-group       MD5  DES  800002a20300fce3900106
john              user-group       SHA  DES  800002a20300fce3900106
```

```console
Console # show snmp users bob
Name          Group Name    Auth Meth     Priv Meth   Remote Engine ID
--------------- --------------- ---- ---- -------------------
bob               user-group       MD5  DES  800002a20300fce3900106
```

### show snmp views

Use the `show snmp views` command to display the configuration of views.
**Syntax**

`show snmp views [viewname]`
- `viewname` — Specifies the name of the view. (Range: 1-30)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following examples display the configuration of views with and without a view name specified.

```
console# show snmp views

Name       OID Tree             Type
----------- ----------------------- --------
user-view1  1.3.6.1.2.1.1       Included
user-view1  1.3.6.1.2.1.1.7     Excluded
user-view2  1.3.6.1.2.1.2.1.*.1 Included
```

**show trapflags**

Use the `show trapflags` command to display the trap settings.

**Syntax**

`show trapflags [vrf {vrf-name}] [ospf | ospfv3 | captive-portal]`
- `vrf-name` — The name of an existing VRF instance.
• **ospf**—Display OSPFv2 specific trap settings.
• **ospfv3**—Display OSPFv3 specific trap settings.
• **captive-portal**—Display captive-portal specific trap settings.

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example #1**

```
c>show trapflags

Authentication Flag......................... Enable
Auto-copy-sw Flag.......................... Enable
Dot1q Flag.................................. Enable
Link Up/Down Flag........................... Enable
Port-security violation Flag............... Enable
Multiple Users Flag........................ Enable
Mbuf Threshold Flag........................ Enable
CPU Threshold Flag........................ Enable
Spanning Tree Flag......................... Enable
PoE Traps.................................. Enable
VRRF trap.................................. Enable
ACL Traps.................................. Enable
BGP Traps.................................... Disable
DVMRP Traps................................ Disable
OSPFv2 Traps................................. Disable
PIM Traps.................................. Disable
OSPFv3 traps................................ Disable
CP Traps.................................... Disable

Example #2

c>show trapflags ospf

OSPFv2 traps............................... Disabled
errors:
    all.................................... Disabled
```
lsa:
  all....................................... Disabled

overflow:
  all....................................... Disabled

retransmit:
  all....................................... Disabled

state-change:
  all....................................... Disabled

snmp-server community

Use the `snmp-server community` command in Global Configuration mode to set the community string to allow access to the switch SNMP MIBs. To remove the specified community string, use the `no` form of this command.

**Syntax**

```
snmp-server community community-string {ro | rw | su} [view view-name] [ip-address ipaddress] [ipmask ip-mask]
```

```
no snmp-server community community-string
```

- **community-string**—The SNMP community identifier. See `SNMP-BASE-MIB` for further information. (Range: 1-20 printable characters other than an at sign, a backslash, or a question mark.)
- **ro**—Indicates read-only access.
- **rw**—Indicates read-write access.
- **su**—Indicates SNMP administrator access.
- **ip-address**—Specifies the IP address or subnet of the management station(s). If no IP address is specified, all management stations are permitted. Both IPv4 and IPv6 addresses are accepted. If a subnet is specified, it may be entered in the form of an IPv4 address and a space, followed by a forward slash, followed by the decimal number of significant bits with intervening space, or the IP address may be followed by an IPv4 mask in dotted quad notation. The range of IPv4 significant bits is 1 to 31 bits.
- **view-name**—Specifies the name of a previously defined view. For information on views, see the User Guidelines below. (Range: 1-30 characters)
**Default Configuration**
No community is defined. Defaults to read–only access if not specified.

**Command Mode**
Global Configuration mode

**User Guidelines**
The @ character is reserved for future use. It is not accepted in a community string. The question mark is the CLI help trigger. It may not be used in a community name. The backslash is a programmatic escape character. It may not be used in a community name.

You cannot specify a view-name for su, which has access to the whole MIB. You can use the view name to restrict the access rights of a community string. When it is specified:

- An internal security name is generated.
- The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
- The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view name. If ro is specified, then read-view and notify-view are mapped. If rw is specified, then read-view, notify-view, and write-view are mapped.

The community name may include any printable characters except a question mark, an at sign, or a backslash. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

**Command History**
Modified in version 6.5 firmware.

**Example**
The following example configures community access string public to permit administrative access to SNMP at an administrative station with IP address 192.168.1.20.

console(config)# snmp-server community public su ipaddress 192.168.1.20
**snmp-server community-group**

Use the `snmp-server community-group` command in Global Configuration mode to map the internal security name for SNMP v1 and SNMP v2 security models to the group name. To remove the specified community string, use the `no snmp-server community` command.

**Syntax**

```
 snmp-server community-group community-string group-name [ip-address]
 no snmp-server community-group community-string
```

- `community-string` — The SNMP community identifier. See SNMP-COMMUNITYMIB (Range: 1-20 printable characters other than an at sign, a backslash, or a question mark.)
- `group-name` — Name of a previously defined group. The group defines the objects available to the community. (Range: 1-30 characters)
- `ip-address` — Specifies the IP address or subnet of the management station(s). If no IP address is specified, all management stations are permitted. Both IPv4 and IPv6 addresses are accepted. If a subnet is specified, it may be entered in the form of an IPv4 address, followed by a space and a forward slash, followed by the decimal number of significant bits with no intervening spaces, or the IP address may be followed by an IPv4 mask in dotted quad notation. The range of IPv4 significant bits is 1 to 31 bits.

**Default Configuration**

No community group is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

The `group-name` parameter can be used to restrict the access rights of a community string. When it is specified, the software:

- Generates an internal security-name.
• Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

The community name may include any printable characters except a question mark, a backslash, or an at sign. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character, or reject the entry entirely.

**Example**

The following example maps a community access string dell_community to group dell_group and restricts access to host 192.168.29.1.

```
console(config)# snmp-server community-group dell_community dell_group
ipaddress 192.168.29.1
```

**snmp-server contact**

Use the `snmp-server contact` command in Global Configuration mode to set up a system contact (sysContact) string. To remove the system contact information, use the `no` form of the command.

**Syntax**

```
snmp-server contact text
no snmp-server contact
```

- `text` — Character string, 1 to 255 characters, describing the system contact information.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command has no user guidelines.
Example

The following example displays setting up the system contact point as “Dell_Technical_Support”.

```
console(config)# snmp-server contact Dell_Technical_Support
```

snmp-server enable traps

Use the `snmp-server enable traps` command in Global Configuration mode to enable sending SNMP traps globally or to enable sending individual SNMP traps. Use the no form of this command to disable sending SNMP traps individually or globally.

Syntax

```
snmp-server enable traps [acl | all | auto-copy-sw | bgp state-changes
limited | buffers | captive-portal cp-type | cpu | dot1q | dvrmp | link | port-
security [trap-rate] | multiple-users | [vrf vrf-name] ospf ospftype | ospfv3
ospfv3type | pim | poe | snmp authentication | spanning-tree | vrrp]
```

```
no snmp-server enable traps [acl | all | auto-copy-sw | bgp state-changes
limited | buffers | captive-portal cp-type | cpu | dot1q | dvrmp | link | port-
security [trap-rate] | multiple-users | [vrf vrf-name] ospf ospftype | ospfv3
ospfv3type | pim | poe | snmp authentication | spanning-tree | vrrp]
```

- `cp-type` — {all, client-auth-failure, client-connect, client-db-full, client-
disconnect}
- `vrf-name`—The name of a VRF instance for OSPF traps.
- `ospftype`— {all | errors {all | authentication failure | bad packet | config error | virt authentication failure | virt bad packet | virt config
error} | lsa {all | lsa-maxage | lsa originate} | overflow {all | lsdb-
overflow | lsdbapproaching-overflow} | retransmit {all | packets | virt-
packets} | state-change {all | if state change | neighbor state change | virtifstate change | virtneighbor state change}}
- `ospfv3type`—{all | errors {all | bad packet | config error | virt bad
packet | virt config error} | lsa {all | lsa-maxage | lsa originate} | overflow {all | lsdb-overflow | lsdbapproaching-overflow} | retransmit
{all | packets | virt-packets} | state-change {all | if state change | neighbor state change | virtif state change | virtneighbor state change}}
- `acl`—Enable traps on ACL match events.
- **all**—Enable all traps (not recommended).
- **auto-copy-sw**—Enable traps on automatic download of switch software.
- **bgp state-changes limited**—Enable the two traps defined in the standard BGP MIB, RFC 4273. A trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.
- **captive-portal**—Enable captive-portal traps.
- **dot1q**—Enable traps on VLAN configuration failures.
- **bgp state-changes limited**—Enable standard traps defined in RFC 4273.
- **port-security**—Enable traps on port security violations.
- **port-security trap-rate**—Configure the interval at which port security traps are issued. Range 1-1000000 seconds. Default 30 seconds.
- **buffers**—Enables sending of a trap on the internal message buffer count exceeding the rising threshold.
- **cpu threshold**—Enables sending of a trap on the CPU occupancy exceeding the rising threshold.
- **multiple-users**—Enable sending a trap when multiple logins are active.
- **link**—Enable sending a trap when a link (interface) transitions to the active state or the inactive state.
- **violation**—Enable sending a trap when a port security MAC locking violation occurs.
- **vrf-name**—The name of an existing VRF instance
- **dvmrp**—Enable DVMRP traps.
- **port-security**—Enable traps on port security violations.
- **ospf**—Enable OSPF event traps.
- **ospfv3**—Enable OSPFv3 event traps.
- **pim**—Enable PIM traps (pim-sm and pim-dm).
- **poe**—Enable PoE traps. This parameter is only available on PoE capable switches.
- **snmp authentication**—Enable SNMP authentication traps.
- **spanning-tree**—Enable traps on topology changes.
- **vrrp**—Enable VRRP traps.
Default Configuration
SNMP authentication, link, multiple-user, spanning-tree, dot1q, and ACL traps are enabled by default. Port-security traps are enabled by default.

Command Mode
Global Configuration mode.

User Guidelines
Use the command with no parameters to globally enable sending of traps. Use the no form of the command with no parameters to globally disable sending of traps without changing the configured traps.

Refer to the description of the global configuration mode buffer command for setting the rising and falling thresholds for the sending of the message buffer trap.

Refer to the description of the Global Configuration mode process cpu command for setting the rising and falling thresholds for the sending of the CPU occupancy trap.

Command History
Introduced in version 6.2.0.1 firmware.

Example
The following example displays the options for the snmp-server enable traps command.

```
console(config)#snmp-server enable traps ?
<cr>                     Press enter to execute the command.
acl                      Enable/Disable traps for access control lists.
all                      Enable/Disable all Traps.
auto-copy-sw             Enable/Disable auto copy of code if there is a version mismatch.
bgp                      Enable BGP traps.
buffers                  Configure Mbuf threshold traps.
captive-portal           Enable/Disable SNMP traps for CP system events.
cpu                      Configure CPU threshold traps.
dot1q                    Enable/Disable switch level Dot1q trap flag.
dvmrp                    Enable/Disable traps for distance vector multicast routing protocol.
```
Switch Management Commands

link                  Enable/Disable switch level Link Up/Down trap flag.
multiple-users       Configure multiple users login traps.
ospf                 Enable/Disable OSPF Traps.
ospfv3               Enable/Disable OSPFv3 Traps.
pim                  Enable/Disable traps for protocol-independent multicast.
port-security        Enable/Disable switch level Maclock Violation trap flag.
snmp                 Enable SNMP traps.
spanning-tree        Configure spanning tree traps.
vrf                  Specify VPN Routing/Forwarding instance.
vrrp                 Enable/Disable VRRP trap.

**snmp-server engineID local**

Use the `snmpserver engineID local` command in Global Configuration mode to specify the Simple Network Management Protocol (SNMP) engine ID on the local device.

To remove the configured engine ID, use the `no` form of this command.

**Syntax**

`snmp-server engineID local {engineid-string | default}`

`no snmp-server engineID local`

- **engineid-string** — The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 6-32 characters)
- **default** — The engineID is created automatically, based on the device MAC address.

**Default Configuration**

The engineID is generated using the switch MAC address.

**Command Mode**

Global Configuration mode
User Guidelines

If you want to use SNMPv3, an engine ID is required for the switch. You can specify your own ID or use the default string that is generated using the MAC address of the device. If the SNMPv3 engine ID is changed, or the configuration file is erased, then SNMPv3 cannot be used until the SNMPv3 users are reconfigured. Since the EngineID must be unique within an administrative domain, the following guidelines are recommended:

1. For standalone devices use the default keyword to configure the Engine ID.
2. For stackable systems, configure your own EngineID, and verify that is unique within your administrative domain.

Changing the value of the snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then deleted and is not stored on the switch, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid and the users will have to be reconfigured.

Example

The following example configures the Engine ID automatically.

```
console(config)# snmp-server engineID local default
```

**snmp-server filter**

Use the `snmp-server filter` command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the `no` form of this command.

**Syntax**

```
snmp-server filter filter-name oid-tree {included | excluded}
no snmp-server filter filter-name [oid-tree]
```

- `filter-name` — Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters.)
Switch Management Commands

oid-tree — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wild card to specify a subtree family; for example, 1.3.*.4.

- included — Indicates that the filter type is included.
- excluded — Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

An SNMP server filter identifies the objects to be included or excluded from notifications sent to a server per RFC 2573 Section 6 "NotificationFiltering." This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

The filter name may include any printable characters except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely. Per RFC 2573, configuring a filter adds an implicit exclude-all as the first entry in a filter record. Unless an include statement is specified, all notifications are excluded by default.

Examples

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

console(config)# snmp-server filter user-filter system included
console(config)# snmp-server filter user-filter system.7 excluded
console(config)# snmp-server filter user-filter ifEntry.*.1 included
**snmp-server group**

Use the `snmp-server group` command in Global Configuration mode to configure a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the `no` form of this command.

**Syntax**

```
snmp-server group groupname { v1 | v2 | v3 { noauth | auth | priv } [ notify notifyview ] } [ context contextname ] [ read readview ] [ write writeview ]
```

```
no snmp-server group groupname { v1 | v2 | v3 { noauth | auth | priv } } [ context contextname ]
```

- `groupname` — Specifies the name of the group. (Range: 1-30 characters.)
- `v1` — Indicates the SNMP Version 1 security model.
- `v2` — Indicates the SNMP Version 2 security model.
- `v3` — Indicates the SNMP Version 3 security model.
- `noauth` — Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- `auth` — Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- `priv` — Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- `contextname` — Provides different views of the system and provides the user a way of specifying that context.
- `notifyview` — Defines a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: 1-30 characters.)
- `readview` — A string that is the name of the view that enables the you to view only the contents of the agent. If unspecified, all the objects except for the community-table and SNMPv3 user and access tables are available. (Range: 1-30 characters.)
• writeview — A string that is the name of the view that enables the user to enter data and configure the contents of the agent. If unspecified, nothing is defined for the write view. (Range: 1-30 characters.)

**Default Configuration**

No group entry exists. There will be some default groups for Read/Write/Super users. These groups cannot be deleted or modified by the user. This command is used only to configure the user-defined groups.

**Command Mode**

Global Configuration Mode

**User Guidelines**

View-name should be an existing view created using the `snmp-server view` command. If there are multiple records with the same view-name, then the argument specified in this command points to first view-name in the table.

**Example**

The following example attaches a group called `user-group` to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called `user-view`.

```
console(config)#snmp-server view user-view iso included
console(config)#snmp-server group user-group v3 priv read user-view
```

**snmp-server host**

Use the `snmp-server host` command in Global Configuration mode to specify the recipient of Simple Network Management Protocol notifications. To remove the specified host, use the `no` form of this command. This command enters the user into SNMP-host configuration mode.

**Syntax**

```
snmp-server host host-addr [informs [timeout seconds] [retries retries] | traps version {1 | 2 }]] community-string [udp-port port] [filter filtername]
no snmp-server host host-addr { traps | informs }
```
• **host-addr**—Specifies the IP address of the host (targeted recipient) or the name of the host. Both IPv4 and IPv6 addresses are accepted. (Range: 1-158 characters)

• **community-string**—Specifies a password-like community string sent with the notification operation. (Range: 1-20 characters). The community-string may include any printable characters except a question mark, a backslash, or an at sign.

• **traps**—Indicates that SNMP traps are sent to this host.

• **version 1**—Indicates that SNMPv1 traps will be used.

• **version 2**—Indicates that SNMPv2 traps will be used.

• **informs**—Indicates that SNMPv2 informs are sent to this host.

• **seconds**—Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1-300.)

• **retries**—Maximum number of times to resend an inform request. The default is 3 attempts. (Range: 1-255)

• **port**—UDP port of the host to use. The default is 162. (Range: 1-65535.)

• **filtername**—A string that is the name of the filter that defines the filter for this host. If unspecified, does not filter anything. (Range: 1-30 characters.)

**Default Configuration**

The default configuration is 3 retries, and 15 seconds timeout. This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host. If no version keyword is present, the default is Version 1.

**Command Mode**

Global Configuration mode
**User Guidelines**

If a DNS host name is entered instead of an IP address, the switch attempts to resolve the host name immediately using DNS. Use the `ip domain-lookup` command and the `ip name-server` command to enable resolution of DNS host names.

**Example**

The following example enables SNMP traps for host 192.16.12.143.

```plaintext
console(config)# snmp-server host 192.16.12.143 Dell EMC Networking traps version 2
```

**snmp-server location**

Use the `snmp-server location` command in Global Configuration mode to set the system location string. To remove the location string, use the `no` form of this command.

**Syntax**

```plaintext
snmp-server location text
no snmp-server location
```

- **text** — Character string describing the system location. (Range: 1 to 255 characters.)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

The location string may contain embedded blanks if enclosed in quotes. Any printable character is allowed in the string.

**Example**

The following example sets the device location as “New_York”.

```plaintext
```
console(config)# snmp-server location New_York

**snmp-server user**

Use the `snmp-server user` command in Global Configuration mode to configure a new SNMP Version 3 user. To delete a user, use the `no` form of this command.

**Syntax**

```plaintext
snmp-server user username groupname [remote engineid-string] [ { auth-md5 password | auth-sha password | auth-md5-key md5-key | auth-sha-key sha-key } [priv-des password | priv-des-key des-key | priv-3des password | priv-3des-key des-key | priv-aes128 password | priv-aes128-key aes-key ] ]

no snmp-server user username
```

- **username** — Specifies the name of the user on the host that connects to the agent. (Range: 1-32 characters.)
- **groupname** — Specifies the name of the group to which the user belongs. (Range: 1-40 characters.)
- **engineid-string** — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. The remote engine id designates the remote management station, and should be defined to enable the device to receive acknowledgments to “informs.” (Range: 5-32 characters.)
- **auth-md5** — HMAC-MD5-96 authentication mode.
- **auth-sha** — HMAC-SHA-96 authentication mode.
- **password** — A password. (Range: 1 to 32 characters.)
- **auth-md5-key** — HMAC-MD5-96 authentication message digest key. Enter a pre-generated MD5 key.
- **auth-sha-key** — HMAC-SHA-96 authentication message digest key. Enter a pre-generated SHA key.
- **md5-key** — Character string—length 32 hex characters.
- **sha-key** — Character string—length 40 hex characters.
- **priv-des** — CBC-DES Symmetric Encryption privacy mode. Enter a shared password to generate the key.
• **priv-des-key** — CBC-DES Symmetric Encryption privacy mode. The administrator should enter a pre-generated DES encryption key.

• **des-key** — The pre-generated DES encryption key. The length is determined by the authentication method selected. Enter 32 hex characters if MD5 Authentication is selected, 40 hex characters if SHA Authentication is selected.

• **priv-3des** — The CBC 3DES Symmetric Encryption privacy level. Enter a shared password to generate the key.

• **priv-3des-key** — The CBC-3DES Symmetric Encryption privacy level. The administrator should enter a pre-generated 3DES key.

• **priv-aes128** — CBC-AES128 Symmetric Encryption privacy mode.

• **priv-aes128-key** — A pre-generated AES128 encryption key - 32 hex characters in length.

• **aes-key** — Advanced Encryption Standard. Enter a pre-generated AES key of the appropriate length (128 or 256 bits). An AES 128 bit key is 32 hexadecimal characters in length.

**Default Configuration**

No user entry exists.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the SNMP local engine ID is changed, configured users will no longer be able to connect and will need to be re-configured (deleted from the configuration and added back).

Use of MD5 authentication in conjunction with AES privacy is discouraged as it results in a weak cypher. Utilize SHA authentication when using AES privacy.

The SNMP group must exist or an error is displayed and the user is not configured. The user name can consist of any printable character and may contain embedded blanks if enclosed in quotes.
Example
The following example configures an SNMPv3 user “John” in group “user-group”.

console(config)# snmp-server user John user-group

**snmp-server view**

Use the **snmp-server view** command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server view entry. To delete a specified SNMP server view entry, use the **no** form of this command.

**Syntax**

**snmp-server view** view-name oid-tree { **included** | **excluded** }

**no snmp-server view** view-name [oid-tree]

- **view-name** — Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters.)

- **oid-tree** — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as `1.3.6.2.4`, or a word, such as `system`. Replace a single subidentifier with the asterisk (*) wild card to specify a subtree family; for example `1.3.*.4`.

- **included** — Indicates that the view type is included.

- **excluded** — Indicates that the view type is excluded.

**Default Configuration**

A view entry does not exist.

**Command Mode**

Global Configuration mode
User Guidelines

A view is a set of ASN.1 objects the SNMP server is allowed to access. Multiple view statements may be entered for a particular view. This command can be entered multiple times for the same view record.

The view name accepts any printable characters except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal combinations of characters on entry and may accept entries up to the first illegal character or reject the entry entirely.

Examples

The following example creates a view named user-view that includes all objects in the MIB-II system group except for sysServices (system.7) and includes all objects for interface 1 in the MIB-II interface group. An additional example of embedded blanks in a view name is given on the last line.

```
console(config)# snmp-server view user-view system included
console(config)# snmp-server view user-view system.7 excluded
console(config)# snmp-server view user-view ifEntry.*.1 included
console(config)#snmp-server view "A beautiful view!" 1.1.2.1 included
```

snmp-server v3-host

Use the `snmp-server v3-host` command in Global Configuration mode to specify the recipient of Simple Network Management Protocol Version 3 (SNMPv3) notifications. To remove the specified host, use the `no` form of this command.

Syntax

```
snmp-server v3-host {ip-address | hostname} username {traps | informs} [noauth | auth | priv] [timeout seconds] [retries retries] [udpport port] [filter filtername]

no snmp-server v3-host ip-address {traps | informs}
```

- ip-address — Specifies the IP address of the host (targeted recipient). Both IPv4 and IPv6 addresses are allowed.
Switch Management Commands

- **hostname** — Specifies the name of the host. (Range: 1-158 characters.) The command allows spaces in the host name when specified in double quotes. For example, `#snmp-server v3-host "host name"`. Note that the switch will not resolve host names that are not in conformance with RFC 1035.

- **username** — Specifies user name used to generate the notification. (Range: 1-30 characters.)

- **traps** — Indicates that SNMP traps are sent to this host.

- **informs** — Indicates that SNMPv2 informs are sent to this host.

- **noauth** — Specifies sending of a packet without authentication.

- **auth** — Specifies authentication of a packet without encrypting it

- **priv** — Specifies authentication and encryption of a packet.

- **seconds** — Number of seconds to wait for an acknowledgment before resending informs. This is not allowed for hosts configured to send traps. The default is 15 seconds. (Range: 1-300 seconds.)

- **retries** — Maximum number of times to resend an inform request. This is not allowed for hosts configured to send traps. The default is 3 attempts. (Range: 0-255 retries.)

- **port** — UDP port of the host to use. The default is 162. (Range: 1-65535.)

- **filtername** — A string that is the name of the filter that define the filter for this host. If unspecified, does not filter anything. (Range: 1-30 characters.)

**Default Configuration**

The default configuration is 3 retries and 15 seconds timeout.

**Command Mode**

Global Configuration mode
**User Guidelines**

The username can include any printable characters except a question mark. Enclose the string in double quotes to include spaces within the key. The surrounding quotes are not used as part of the key. The CLI does not filter illegal characters but may accept entries up to the first illegal character or reject the entry entirely.

**Example**

The following example configures an SNMPv3 host, and sets it to send SNMP INFORMS with user name John using authentication without encryption.

```
console(config)# snmp-server v3-host 192.168.0.20 John informs auth
```

The following example shows the syntax of the no snmp-server host ip-address command.

```
console(config)#no snmp-server host 1.2.3.4 ?
```

- `informs` Sends SNMP informs to this host.
- `traps` Sends SNMP traps to this host.

**Command History**

Example updated in 6.4 release.

**snmp-server source-interface**

Use the `snmp-server source-interface` command to select the interface from which to use the IP address in the source IP address field of transmitted SNMP traps and informs. Use the `no` form of the command to revert to the default IP address.

**Syntax**

```
snmp-server source-interface { loopback loopback-id | vlan vlan-id }

no snmp-server source-interface
```

- `loopback-id` — A loopback interface identifier.
- `vlan-id` — A VLAN identifier.
**Default Configuration**

By default, the switch uses the assigned switch IP address as the source IP address for SNMP packets. This is either the IP address assigned to the VLAN from which the SNMP packet originates or the out-of-band interface IP address.

**Command Mode**

Global Configuration

**User Guidelines**

The source interface must have an assigned IP address (either manually or via another method such as DHCP). This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```bash
console#conf
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#snmp-server source-interface vlan 1
```
SupportAssist Commands

The commands in this section enable configuration of SupportAssist.

Commands in this Section

This section explains the following commands:

- **eula-consent**
  - **Syntax**:
    - `eula-consent
      
      {support-assist} {accept | reject}
    
    - **support-assist**—Enter the keyword support-assist to either accept or reject the EULA for the SupportAssist service.
    
    - **accept** — Accepts the EULA for the specified service.
    
    - **reject** — Rejects the EULA for the specified service.
  
  
  - **Default Configuration**
    - The default is `eula-consent support-assist accept`.
  
  - **Command Mode**
    - Global Configuration
User Guidelines

Messages are shown for both the accept and reject use cases with information directing the user to URLs for further information. If the user rejects or has not yet accepted the EULA, the configuration mode for the specified service will not be usable. If there is existing configuration for that feature, the configuration will not be removed but the feature will be disabled.

This command can be executed multiple times. It overwrites the previous information each time. The collected information is stored in the running-config. The administrator must write the configuration in order to persist it across reboots.

Command History

Introduced in version 6.3.0.1 firmware.

Example

Example 1

```
console(config)# 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. 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: http://www.dell.com/aeula, you agree to allow Dell to provide remote monitoring services of your IT environment and you give Dell the right to collect the Collected Data in accordance with Dell’s Privacy Policy, available at: http://www.dell.com/privacypolicycountryspecific, in order to enable the performance of all of the various functions of SupportAssist during your entitlement to receive related repair services from Dell. You further agree to allow Dell to transmit and store the Collected Data from SupportAssist in accordance with these terms. You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dell's 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.

Example 2
console(config)# eula-consent support-assist reject

I do not accept the terms of the license agreement. The SupportAssist feature has been deactivated and can no longer be used.
To enable SupportAssist configurations, accept the terms of the license agreement by configuring this command 'eula-consent support-assist accept'.

contact-company

Use the contact-company command to configure the contact information to be sent to the SupportAssist server. Use the no form of the command to remove the contact information.

Syntax

contact-company name company street-address streetaddress address city city country country postcode postcode

• company — The company for the technical contact person. Maximum of 256 printable characters.
• streetaddress — The street address for the technical contact person. Maximum of 99 printable characters.
• city — The city for the technical contact person. Maximum of 99 printable characters.
• country — The country for the technical contact person in Alpha-3 format-3 capital-case characters.
• postcode — The postal code for the technical contact person. Maximum of 10 printable characters.

Enclose a parameter in quotes if an embedded blank is desired in the parameter.

Default Configuration

No contact company information is populated by default.
**Command Mode**
Support Assist Configuration

**User Guidelines**
This information is transmitted to Dell if the SupportAssist service is enabled.

This command can be executed multiple times. It overwrites the previous information each time. The collected information is stored in the running-config. The administrator must write the configuration in order to persist it across reboots.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
console(config)# support-assist
console(conf-support-assist)#contact-company name "Dell Inc." street-address "5 Round Rock Way" city "Round Rock, TX" country USA postcode 78665

**contact-person**
Use the `contact-person` command to configure the contact information to be sent to the SupportAssist server. Use the `no` form of the command to remove the contact information.

**Syntax**
```plaintext
contact-person first firstname last lastname email-address primary emailaddress phone phone-number preferred-method { email | phone }
no contact-person
```
- `firstname` — The first name of the technical contact person. Maximum of 50 printable characters.
- `lastname` — The last name of the technical contact person. Maximum of 50 printable characters.
- `email-address primary`—The primary email address of the technical contact. Maximum of 50 printable characters.
• **phone**—The complete phone number. Maximum of 23 printable characters.

• **preferred-method**—The preferred method of contact. May be either email or phone.

**Default Configuration**
No contact person information is populated by default.

**Command Mode**
Support Assist Configuration

**User Guidelines**
The email address must conform to RFC 5322 sections 3.2.3 and 3.4.1 and RFC 5321. Additionally, the character set is further restricted to ASCII characters.

This information is transmitted to Dell if the SupportAssist service is enabled.

This command can be executed multiple times. It overwrites the previous information each time. The collected information is stored in the running-config. The administrator must write the configuration in order to persist it across reboots.

**Command History**
Introduced in version 6.3.0.1 firmware.

**Example**
The following example

```
console(config)# support-assist
console(conf-support-assist)#contact-person first john last doe email-address primary jdoe@mycompany.com phone +1-555-999-9999 preferred-method email
```

**enable**
Use the `enable` command to enable a SupportAssist server. Use the `no` form of the command to disable a SupportAssist server.
Syntax
enable
no enable

Default Configuration
By default, the default server is enabled. It may be disabled using the no enable form of the command.

Command Mode
Support Assist Configuration

User Guidelines
Only one SupportAssist server may be enabled. If contact with the server fails, the switch sleeps for the quiet period (default 1 hour) before attempting contact again.

Command History
Introduced in version 6.3.0.1 firmware.

Example
console(config)# support-assist
console(conf-support-assist)#server New-Server
console(conf-support-assist-NewServer)#enable

proxy-ip-address
Use the proxy-ip-address command to configure a proxy server to be used to contact the SupportAssist servers. Use the no form of the command to remove the proxy server information.

Syntax
proxy-ip-address {ipv4-address | ipv6-address} port port-number username userid password [encryption-type] password
no proxy-ip-address

- ipv4-address — The IPv4 address of the proxy server in dotted decimal notation.
Switch Management Commands

- ipv6-address — The IPv6 address of the proxy server in IPv6 notation.
- port-number — The TCP port number of the proxy server. Range 1-65535. Default 443.
- userid — The user name used to log into the proxy server.
- encryption-type — 0 indicates an unencrypted password. 7 indicates an encrypted password.
- password — An unencrypted or encrypted password. Maximum length is 64 characters for an unencrypted password. Encrypted passwords must be 128 characters in length.

Default Configuration

By default, no proxy is configured.

By default, passwords are entered as unencrypted and are always displayed and stored encrypted.

Command Mode

Support Assist Configuration

User Guidelines

Passwords are always stored and displayed as encrypted, even if entered in unencrypted format.

Command History

Introduced in version 6.3.0.1 firmware.

server

Use the server command to configure a SupportAssist server and enter SupportAssist server configuration mode. Use the no form of the command to remove a SupportAssist server.

server server-name

no server server-name
- server-name — The server name has a maximum length of 20 characters. Any printable character may be used in the server name other than a question mark. Enclose the server name in quotes if an embedded blank is desired in the server name.

Default Configuration
A default server named “default” exists at URL stor.g3.ph.dell.com. This server is pre-configured and may not be removed or modified other than to disable it.

Command Mode
Support Assist Configuration

User Guidelines
The server-name is used as a reference only and is not required to be used as part of a URL definition.
Up to four additional servers may be configured.
Use the exit command to exit from Support Assist Server configuration mode.

Command History
Introduced in version 6.3.0.1 firmware.

Example
```
console(config)# support-assist
console(conf-support-assist)#server default
console(conf-support-assist-default)#
```

**show eula-consent support-assist**
Use the show eula-consent to may be used to review the EULA details whenever desired. Displaying the EULA details does not modify the current state of EULA acceptance for that feature.

**Syntax**
```
show eula-consent support-assist
```
**Default Configuration**

The SupportAssist EULA is Accepted by default.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

Acceptance of the SupportAssist EULA is enabled by default.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#show eula-consent support-assist
SupportAssist EULA has been: Accepted
Additional information about the SupportAssist EULA is as follows:

By installing SupportAssist, you allow Dell to save your contact information (e.g. name, phone number and/or email address) which would be used to provide technical support for your Dell products and services. Dell may use the information for providing recommendations to improve your IT infrastructure. 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: http://www.dell.com/aeula, you agree to allow Dell to provide remote monitoring services of your IT environment and you give Dell the right to collect the Collected Data in accordance with Dell's Privacy Policy, available at: http://www.dell.com/privacypolicycountryspecific, in order to enable the performance of all of the various functions of SupportAssist during your entitlement to receive related repair services from Dell. You further agree to allow Dell to transmit and store the Collected Data from SupportAssist in accordance with these terms. You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dell's 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.

**show support-assist status**

Use the `show support-assist status` command to display information on
SupportAssist feature status including any activities, status of
communication, last time communication sent, etc.

**Syntax**

`show support-assist status`

**Default Configuration**

This command has no defaults.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration
submodes

**User Guidelines**

There are no guidelines for this command.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console# show support-assist status
SupportAssist: Enabled
SupportAssist Server: https://stor.g3.ph.dell.com (resolved)
EULA: Accepted
Proxy Server: 172.167.33.101

<table>
<thead>
<tr>
<th>Activity</th>
<th>State</th>
<th>Last Start</th>
<th>Last Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy port</td>
<td>8080</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Success</td>
<td>MM/DD/YYYY</td>
<td>HH:mm:ss AM</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td>MM/DD/YYYY</td>
<td>HH:mm:ss AM</td>
</tr>
<tr>
<td>Full Transfer</td>
<td>Success</td>
<td>MM/DD/YYYY</td>
<td>HH:mm:ss AM</td>
</tr>
</tbody>
</table>
```
support-assist

Use the support-assist command to enable support-assist configuration mode if the EULA has been accepted. Use the no form of the command to remove the configured SupportAssist information.

Syntax

support-assist
no support-assist

Default Configuration

By default, a server named “default” is configured. It may be disabled by the administrator.

Command Mode

Global Configuration

User Guidelines

This command enters support-assist-conf mode. It allows the administrator to configure SupportAssist information. The configured information is stored in the running config. Use the write command to save the information into the startup-config.

Command History

Introduced in version 6.3.0.1 firmware.

Examples

Example 1

In this example, the SupportAssist EULA has been accepted.

```
console(config)#support-assist
console(conf-support-assist)#
```

Example 2

In this example, the SupportAssist EULA has been rejected.

```
console(config)#support-assist
```
SupportAssist EULA has not been accepted.
SupportAssist cannot be configured until the SupportAssist EULA is accepted.

console(config)#

**url**

Use the `url` command to configure the URL to reach on the SupportAssist remote server. Use the `no` form of the command to remove the URL information.

**Syntax**

`url uniform-resource-locator`

`no url`

`uniform-resource-locator` — A text string for the URL using one of the following formats:
```
http://[username:password@]<hostip>:<portNum>/<filepath>
https://[username:password@]<hostip>:<portNum>/<filepath>
```

**Default Configuration**

By default, no URL is configured.

**Command Mode**

Support Assist Configuration

**User Guidelines**

The hostip 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 feature will need to be configured, enabled and operational.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```console
console(config)# support-assist
console(conf-support-assist)#server default
```
console(config) support-assist
console(config-support-assist)# server new
console(config-support-assist-new)# url https://stor.g3.ph.dell.com
SYSLOG Commands

The Dell EMC Networking supports a centralized logging service with support for local in-memory logs, crash dump logs, and forwarding messages to SYSLOG servers. All switch components use the logging service. Components log messages to the logging component using one of the following severity levels:

- Emergency (0): system is unusable
- Alert (1): action must be taken immediately
- Critical (2): critical conditions
- Error (3): error conditions
- Warning (4): warning conditions
- Notice (5): normal but significant conditions
- Informational (6): informational messages
- Debug (7): debug-level messages

Command Logging

The Dell EMC Networking Command Logging component logs all command line interface commands issued on the system. The command log messages are stored with the other system logs and provide the system operators with a detailed log of the commands executed.

CLI command logging is configured through any of the Dell EMC Networking management interfaces. When the feature is enabled, all CLI commands are logged using the existing logging service. By default, CLI command logging is disabled.

Dell EMC Networking supports both RFC 3164 and RFC 5424 logging to remote SYSLOG servers.

The CLI command logging severity is set to SEVERITY_NOTICE. The command logging severity is not modifiable by the administrator.

For example, the CLI log message for the user admin is:

```
<189> Oct 24 02:10:32 10.27.23.197-1 CMDLOGGER[emWeb]: cmd_logger_api.c(83)
440 % NOTE CLI:EIA-232::show run
<189> Oct 24 02:10:28 10.27.23.197-1 CMDLOGGER[emWeb]: cmd_logger_api.c(83)
439 % NOTE CLI:EIA-232::exit
```
If enabled, the CLI command logger subsystem begins to log commands immediately after the user is authenticated. After authentication, the CLI generates an explicit message and invokes the command logger. The format of the message at login is:

```
<189> Oct 24 02:10:26 10.27.23.197-1 CMDLOGGER[emWeb]: cmd_logger_api.c(83)
438 % NOTE CLI:EIA-232::logging buffered info
```

The CLI command log subsystem also logs all user log out instances. The format of the log message is:

```
<190> Jan 10 18:58:56 10.27.21.22-2 CMDLOGGER[209809328]:
    cmd_logger_api.c(260) 362 % INFO [CLI:admin:10.27.21.22] User has successfully logged in
```

### Commands in this Section

This section explains the following commands:

| clear logging | logging monitor |
| clear logging file | logging on |
| description (Logging) | logging protocol |
| level | logging protocol |
| logging cli-command | logging snmp |
| logging | logging source-interface |
| logging audit | logging traps |
| logging buffered | logging web-session |
| logging console | port |
| logging facility | show logging |
| logging file | show logging file |
| — | show syslog-servers |
| terminal monitor | |
**clear logging**

Use the `clear logging` command to clear messages from the internal logging buffer.

**Syntax**

clear logging

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example clears messages from the internal SYSLOG message logging buffer.

```
console#clear logging
Clear logging buffer [y/n]
```

**clear logging file**

Use the `clear logging file` command to clear messages from the logging file.

**Syntax**

clear logging file

**Default Configuration**

There is no default configuration for the command.

**Command Mode**

Privileged Exec
User Guidelines

This command has no user guidelines.

Example

The following example shows the clear logging file command and confirmation response.

console#clear logging file
Clear logging file [y/n]

description (Logging)

Use the description command in Logging mode to describe the SYSLOG server.

Syntax

description description
  • description — Sets the description of the SYSLOG server. (Range: 1-64 characters.)

Default Configuration

This command has no default value.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific SYSLOG server, the command can be executed to set the description of the server.

Example

The following example sets the SYSLOG server description.

console(config logging)#description "syslog server 1"
**level**

Use the **level** command in Logging mode to specify the severity level of SYSLOG messages. To reset to the default value, use the **no** form of the command.

**Syntax**

level <level>

no level

- level—The severity level for SYSLOG messages. (emergencies, alerts, critical, errors, warnings, notifications, informational, debugging)

**Default Configuration**

The default value for level is **info**.

**Command Mode**

Logging mode

**User Guidelines**

After entering the view corresponding to a specific SYSLOG server, the command can be executed to set the severity level for SYSLOG messages. Debug level messages are intended for use by support personnel. The output is voluminous, cryptic, and because of the large number of messages generated, can adversely affect switch operations. Only set the logging level to debug under the direction of support personnel.

**Example**

The following example sets the SYSLOG message severity level to alert.

```console
console(config-logging)#level alerts
```

**logging cli-command**

Use the **logging cli-command** in Global Configuration mode to enable CLI command logging.
**Syntax**

logging cli-command
no logging cli-command

**Default Configuration**

Disabled

**Command Mode**

Global Configuration

**User Guidelines**

See the CLI commands by using the `show logging` command.

**Example**

```plaintext
console(config)#logging cli-command
console(config)#do show logging

console#show logging

Logging is enabled
Logging protocol version: 0
Source Interface......................... Default
Console Logging: Level warnings. Messages : 3 logged, 320 ignored
Monitor Logging: disabled
Buffer Logging: Level informational. Messages : 55 logged, 268 ignored
File Logging: Level emergencies. Messages : 0 logged, 323 ignored
Switch Auditing : enabled
CLI Command Logging: disabled
Web Session Logging : disabled
SNMP Set Command Logging : disabled
Logging facility level : local7
0 Messages dropped due to lack of resources
Buffer Log:
<189> Jan 10 18:59:09 10.27.21.22-2 CMDLOGGER[209809328]: cmd_logger_api.c(83) 367 % NOTE CLI:EIA-232:----:configure
<190> Jan 10 18:59:17 10.27.21.22-2 CLI_WEB[209809328]: cmd_logger_api.c(260) 369 % INFO [CLI:----:EIA-232] Access level of user admin has been set to 15
<189> Jan 10 18:59:19 10.27.21.22-2 CMDLOGGER[209809328]: cmd_logger_api.c(83) 370 % NOTE CLI:EIA-232:----:exit
<189> Jan 10 18:59:22 10.27.21.22-2 CMDLOGGER[209809328]: cmd_logger_api.c(83) 371 % NOTE CLI:EIA-232:----:telnet 10.27.21.22
```
logging

Use the `logging` command in Global Configuration mode to log messages to a SYSLOG server. To delete the SYSLOG server with the specified address from the list of SYSLOG servers, use the `no` form of this command.

**Syntax**

```
logging {ip-address | ipv6-address | hostname} [tls {anon | x509 | x509 certificate index}]
```

```
no logging {ip-address | ipv6-address | hostname}
```

- `ip-address` — IP address of the host to be used as a SYSLOG server.
- `ipv6-address` — IPv6 address of the host to be used as a SYSLOG server.
- `hostname` — Hostname of the host to be used as a SYSLOG server. (Range: 1-63 characters) The command allows spaces in the host name when specified in double quotes. For example, `#snmp-server v3-host "host name"`.
- `anon`—Use anonymous authentication (that is, anonymous mode with no authentication).
- `x509`—Use mutual authentication (both client and server side). An optional certificate index can be used to identify a specific server and client certificate pair.

**Default Configuration**

When enabling x509 authentication, a default (non-indexed) certificate pair is used if present and no certificate index has been specified.

The default SYSLOG server port number is 514. When DTLS is configured (logging protocol 1), the default port number is 6514.
**Command Mode**

Global Configuration mode

**User Guidelines**

A signed X509 certificate must be present on the switch in order for DTLS (logging protocol 1) to operate. See the `crypto` commands for further information on certificates.

Up to eight SYSLOG servers can be configured.

The Dell EMC Networking uses the local7(23) facility in the SYSLOG message by default. SYSLOG messages will not exceed 96 bytes in length. SYSLOG protocol version 0 messages use the following format:

```
<190> Jan 01 00:00:06 0.0.0.0-1 General[fp_main_task]: bootos.c(191) 4 % INFO Event(0xaaaaaaaa)
```

**Table:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRI</td>
<td>This consists of the facility code (see RFC 3164) multiplied by 8 and added to the severity. See below for more information on severity.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The system up time. For systems that use SNTP, this is UTC. When time zones are enabled, local time will be used.</td>
</tr>
<tr>
<td>Host IP Address or Host Name</td>
<td>The IP address or Host Name of the local system.</td>
</tr>
</tbody>
</table>
Example

The following example configures the named server as an available SYSLOG server.

console# logging Syslog-server-1.dell.com

logging audit

Use the logging audit command to enable switch auditing. Use the no form of the command to disable switch auditing.

Syntax

logging audit
no logging audit

Default Configuration

The command default is enabled.
**Command Mode**
Global Configuration

**Example**
console(config)#logging audit

**logging buffered**
Use the `logging buffered` command in Global Configuration mode to limit SYSLOG messages displayed from an internal buffer based on severity. To cancel the buffer use, use the `no` form of this command.

**Syntax**

```
logging buffered [severity-level]
no logging buffered
```

- `severity-level`—(Optional) The number or name of the desired severity level. Range:
  - [0 | emergencies]
  - [1 | alerts]
  - [2 | critical]
  - [3 | errors]
  - [4 | warnings]
  - [5 | notifications]
  - [6 | informational]
  - [7 | debugging]

**Default Configuration**
The default value for level is `informational`.

**Command Mode**
Global Configuration mode
User Guidelines

All the SYSLOG messages are logged to the internal buffer. This command limits the commands displayed to the user. Debug level messages are intended for use by support personnel. The output is voluminous, cryptic, and because of the large number of messages generated, can adversely affect switch operations. Only set the logging level to debug under the direction of support personnel.

Example

The following example limits SYSLOG messages collected in the internal buffer to those of severity level “error” and above (numerically lower).

```
console(config)#logging buffered error
```

logging console

Use the `logging console` command in Global Configuration mode to limit messages logged to the console based on severity. To disable logging to the console terminal, use the `no` form of this command.

Syntax

logging console [severity–level]

no logging console

- severity–level—(Optional) The number or name of the desired severity level. Range:
  - [0 | emergencies]
  - [1 | alerts]
  - [2 | critical]
  - [3 | errors]
  - [4 | warnings]
  - [5 | notifications]
  - [6 | informational]
  - [7 | debugging]
Default Configuration
The default console logging severity is **emergencies**.

**Command Mode**
Global Configuration mode

**User Guidelines**
Messages at the selected level and above (numerically lower) are displayed on the console. Debug level messages are intended for use by support personnel. The output is voluminous, cryptic, and because of the large number of messages generated, can adversely affect switch operations. Only set the logging level to debug under the direction of support personnel.

**Example**
The following example limits messages logged to the console based on severity level “alerts”.

```
console(config)#logging console alerts
```

**logging facility**
Use the **logging facility** command in Global Configuration mode to configure the facility to be used in log messages.

**Syntax**
logging facility facility
no logging facility

- facility—The facility that will be indicated in the message. (Range: local0, local1, local2, local3, local4, local5, local6, local7).

**Default Configuration**
The default logging facility is local7.

**Command Mode**
Global Configuration mode
**User Guidelines**
This command has no user guidelines.

**Example**
The following example sets the logging facility as `local3`.

`console(config)#logging facility local3`

**logging file**
Use the `logging file` command in Global Configuration mode to limit SYSLOG messages sent to the logging file based on severity. To set the default logging level, use the `no` form of this command.

**Syntax**
`logging file` [severity–level-number | type]
`no logging file`

- `severity–level`—(Optional) The number or name of the desired severity level. Range:
  - `[0 | emergencies]`
  - `[1 | alerts]`
  - `[2 | critical]`
  - `[3 | errors]`
  - `[4 | warnings]`
  - `[5 | notifications]`
  - `[6 | informational]`
  - `[7 | debugging]`

**Default Configuration**
The default severity level is `emergencies`.

**Command Mode**
Global Configuration mode
**User Guidelines**

Debug level messages are intended for use by support personnel. The output is voluminous, cryptic, and because of the large number of messages generated, can adversely affect switch operations. Only set the logging level to debug under the direction of support personnel.

**Example**

The following example limits SYSLOG messages stored in the logging file to severity level “warnings” and above (numerically lower).

```
console(config)#logging file warnings
```

**logging monitor**

Use the `logging monitor` command in Global Configuration mode to enable logging messages to telnet and SSH sessions with the default severity level. Use the `no logging monitor` command to disable logging messages.

**Syntax**

```
logging monitor severity
no logging monitor
```

- severity—(Optional) The number or name of the desired severity level. Range:
  - [0 | emergencies]
  - [1 | alerts]
  - [2 | critical]
  - [3 | errors]
  - [4 | warnings]
  - [5 | notifications]
  - [6 | informational]
  - [7 | debugging]
Default Configuration
The default logging monitor severity level is warnings. By default, logging messages are not displayed on SSH or telnet sessions (no logging monitor warnings). Logging messages are displayed by default on console sessions (serial and out-of-band ports).

Command Mode
Global Configuration mode

User Guidelines
Messages logged to the console are filtered based on severity. Selecting a severity level will log that severity and higher (numerically lower) level messages.

logging on
Use the logging on command in Global Configuration mode to control error messages logging. This command globally enables the sending of logging messages to the currently configured locations. To disable the sending of log messages, use the no form of this command.

Syntax
logging on
no logging on

Default Configuration
Logging is enabled.

Command Mode
Global Configuration mode

User Guidelines
The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or SYSLOG server. Logging on and off for these destinations can be individually
configured using the `logging buffered`, `logging file`, and `logging server` global configuration commands. However, if the `logging on` command is disabled, no messages are sent to these destinations. In this case, only the console will continue to receive logging messages.

**Example**
The following example shows how logging is enabled.

```
console(config)#logging on
```

### logging protocol

Use this command to log messages in RFC5424 format, including time zone and subsecond resolution time stamps. Use the `no` form of this command to set the logging to the default format.

**Syntax**

```
logging protocol {protocol-selector}
no logging protocol
```

- **protocol-selector**—One of the following:
  - 0 – Generate RFC3164 format messages
  - 1 – Generate RFC5424 format messages

**Default Configuration**

Messages are logged in RFC3164 format by default (logging protocol 0).

**Command Modes**

Global Configuration mode.

**User Guidelines**

During system startup, messages are logged in RFC3164 format (e.g., in the startup persistent log). Messages are logged in the selected format upon the system processing the startup configuration.

The time zone must be configured for the system to generate RFC5424 log messages with the time zone included.
**Example**

This example sets the logging message format to RFC5424. DTLS is used for X509 configured SYSLOG servers if a certificate is available.

```
console(config)#logging protocol 1
```

This example sets the logging message format to RFC3164

```
console(config)#no logging protocol
```

The following example shows the logging format when logging protocol is set to 0.

```
console(config)#logging protocol 0
```

```
<190> Oct 18 07:09:15 0.0.0.0-1 RADIUS[radius_task]: radius_api.c(10450) 58 %% INFO RADIUS: Sending RADIUS server state change event to interested users: 1
<189> Oct 18 07:09:15 0.0.0.0-1 TRAPMGR[trapTask]: traputil.c(721) 26 %% NOTE Unit 1 is the new stack master, Old stack master unit is 0
```

The following example shows the logging format when logging protocol is set to 1.

```
console(config)#logging protocol 1
```

```
<190>1 2017-10-18T07:09:23.446Z dhcp-10-130-182-178 UNITMGR cmgrInsertTask unitmgr.c(8063) 232 [stk@674 unit:1][sev@674 INFO] %% No Potential unit to configure as Standby when unit 1 joined
<189>1 2017-10-18T07:09:23.445Z dhcp-10-130-182-178 USB_FD emWeb usbFlashDrive_core.c(903) 231 [stk@674 unit:1][sev@674 NOTE] %% There is startup-config on flash.
<190>1 2017-10-18T07:09:23.432Z dhcp-10-130-182-178 AUTO_INST emWeb auto_install_control.c(1358) 230 [stk@674 unit:1][sev@674 INFO] %% AutoInstall is stopped.
```

The following example shows the logging format when logging protocol is set to 1 with timezone configured on the switch.

```
console(config)#clock timezone +5 minutes 30 zone IST
```

```
console(config)#show clock
```

```
02:17:44 IST(UTC+5:30) Dec 21 2014
Time source is Local

console(config)#
```
logging snmp

Use the logging snmp command in Global Configuration mode to enable SNMP Set command logging. To disable, use the no form of this command.

Syntax

logging snmp
no logging snmp

Default Configuration

By default, logging snmp is disabled.

Command Mode

Global Configuration mode

User Guidelines

To see SNMP Set command logs use the show logging command.

Example

console(config)#logging snmp

logging source-interface

Use the logging source-interface command to select the interface from which to use the IP address in the source IP address field of transmitted SYSLOG packets. Use the no form of the command to revert to the default IP address.

Syntax

logging source-interface {loopback loopback-id} | {tunnel tunnel-id} | {vlan vlan-id} | {out-of-band }
no logging source-interface

• loopback-id — The name of a loopback interface.
• tunnel-id — The name of a tunnel-id.
- **vlan-id** — A VLAN identifier.
- **out-of-band** — The out-of-band interface identifier.

**Default Configuration**

By default, the switch uses the assigned switch IP address. This is either the IP address assigned to VLAN or the out-of-band interface IP address.

**Command Mode**

Global Configuration

**User Guidelines**

This command is not supported on Dell EMC N1100-ON switches. Dell EMC N1100-ON switches support configuration of a single IP address in interface vlan configuration mode. That IP address is used as the source interface address for this function.

**Command History**

Introduced in version 6.3.0.1 firmware.

**Example**

```
console#conf
console(config)#interface vlan 1
console(config-if-vlan1)#ip address dhcp
console(config-if-vlan1)#exit
console(config)#logging source-interface vlan 1
```

**logging traps**

Use the `logging traps` command in Global Configuration mode to set the lowest severity level at which SNMP traps are logged. To revert the urgent severity level to its default value, use the `no` form of this command.

**Syntax**

```
logging traps severity
no logging traps
```
• severity—If you specify a severity level, log messages at or above the severity level are e-mailed. The severity level may either be specified by keyword or as an integer from 0 to 7. The accepted keywords, and the numeric severity level each represents, are as follows.
  – emergency (0)
  – alert (1)
  – critical (2)
  – error (3)
  – warning (4)
  – notice (5)
  – info (6)
  – debug (7)

**Default Configuration**
The default severity level is info(6).

**Command Mode**
Global Configuration mode

**User Guidelines**
You can filter log messages that appear in the buffered log by severity level. You can specify the severity level of log messages that are e-mailed. You can use this command to specify the severity level at which SNMP traps are logged, and thus control whether traps appear in the buffered log or are e-mailed and, if they are e-mailed, whether traps are considered urgent or non-urgent.

**logging web-session**
Use the `logging web-session` command in Global Configuration mode to enable web session logging. To disable, use the no form of this command.

**Syntax**
logging web-session
no logging web-session

**Default Configuration**
Disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
To see web session logs use the show logging command.

**Example**
```
console(config)#logging web-session
<133> Jan 12 13:51:55 10.130.185.29-6 CLI_WEB[emWeb]: cmd_logger_api.c(140) 9788 %% NOTE WEB:10.130.65.150:admin:session[0] created

<133> Jan 12 13:51:55 10.130.185.29-6 CLI_WEB[emWeb]: cmd_logger_api.c(140) 9789 %% NOTE WEB:10.130.65.150:admin:User admin logged in
```

**port**
Use the `port` command in Logging Configuration mode to specify the port number of a SYSLOG server to which SYSLOG messages are sent. To reset to the default value, use the `no` form of the command.

**Syntax**
```
port port
no port
```
- port—The port number to which SYSLOG messages are sent. (Range: 1-65535)

**Default Configuration**
The default port number for UDP messages is 514. When DTLS is configured (logging protocol 1), the default port number is 6514.

**Command Mode**
SYSLOG server configuration mode
User Guidelines
After entering the view corresponding to a specific SYSLOG server, the command can be executed to set the port number for the server. If the port value is changed for a server, the configuration does not take effect until the server is disconnected and reconnected.

Example
The following example sets the SYSLOG server port to 300.

console(config-logging)#port 300

show logging
Use the show logging command to display all logging information, including auditing status and logging protocol version.

Syntax
show logging

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Command History
Updated output in version 6.5.

Example
The following example displays the state of logging and the SYSLOG messages stored in the internal buffer.

console#show logging
Logging is enabled
Logging protocol version: 1
Source Interface............................... out-of-band
Console Logging: Level debugging. Messages : 1221 logged, 8500 ignored
Monitor Logging: disabled
Buffer Logging: Level informational. Messages : 744 logged, 8494 ignored
File Logging: Level emergencies. Messages : 0 logged, 9800 ignored
Switch Auditing : enabled
CLI Command Logging: disabled
Web Session Logging : disabled
SNMP Set Command Logging : disabled
Logging facility level : local7

SYSLOG Server Details:

0.0.0.0 : Level informational. Messages : 0 dropped
0 Messages dropped due to lack of resources
Buffer Log:
<186> Oct 18 07:09:12 0.0.0.0-1 General[fp_main_task]: bootos.c(191) 10 %
CRIT Event(0xaaaaaaaa)
<189> Oct 18 07:09:12 0.0.0.0-1 BSP[fp_main_task]: bootos.c(175) 9 %
NOTE
BSP initialization complete, starting switch firmware.
<190> Oct 18 07:09:12 0.0.0.0-1 OSAPI[fp_main_task]: osapi_crash.c(1297) 8 %
INFO Oldest crashlog (5) will be deleted if another crash happens.
<190> Oct 18 07:09:12 0.0.0.0-1 OSAPI[fp_main_task]: osapi_crash.c(1292) 7 %
INFO 5 Crashlogs found.
<190> Oct 18 07:09:11 0.0.0.0-1 DRIVER[fp_main_task]:
broad_hpc_stacking.c(1236) 6 %
INFO Configuring CPUTRANS RX
<190> Oct 18 07:09:11 0.0.0.0-1 DRIVER[fp_main_task]:
broad_hpc_stacking.c(1224) 5 %
INFO Configuring CPUTRANS TX
<190> Oct 18 07:09:11 0.0.0.0-1 DRIVER[fp_main_task]:
broad_hpc_stacking.c(1193) 4 %
INFO Adding BCM transport pointers
<189> Oct 18 07:09:06 0.0.0.0-1 General[fp_main_task]:
sdm_template_mgr.c(488) 3 %
NOTE Booting with default SDM template Data
Center - IPv4 and IPv6.
<190> Oct 18 07:09:05 0.0.0.0-1 General[procLOG]: procmgr.c(3685) 2 %
INFO Application Terminated (user.start, ID = 7, PID = 1349
<185> Oct 18 07:09:05 0.0.0.0-0 General[fp_main_task]: unitmgr.c(6612) 1 %
ALRT Reboot 1 (0x1)

A protocol version 1 message will appear as follows:

<189>1 2017-10-18T07:09:22.796Z dhcp-10-130-182-178 TRAPMGR trapTask - :
traputil.c(721) 222 [stk@674 unit:1] [sev@674 NOTE]% Link on V11 is failed
show logging file

Use the show logging file command to display the state of logging and the messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging messages sorted in the logging file.

```
console(config)#show logging file
Persistent Logging : enabled
Persistent Log Count : 0

--------------------------------------------------------------------------
Persistent Log File Empty
```

show syslog-servers

Use the show syslog-servers command to display the SYSLOG servers settings.

Syntax

show syslog-servers
Default Configuration
When enabling x509 authentication, a default (non-indexed) certificate pair is used if present and no index was selected for the server.
Anonymous authentication does not use a certificate.
The default SYSLOG server port number is 514. When DTLS is configured (logging protocol 1), the default port number is 6514.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command has no user guidelines.

Example
The following example displays the SYSLOG server settings.

```
console#show syslog-servers
```

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.180.2.275</td>
<td>14</td>
<td>Info</td>
<td>7</td>
</tr>
<tr>
<td>192.180.2.285</td>
<td>14</td>
<td>Warning</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transport Type</th>
<th>Authentication</th>
<th>Certificate Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td>X509</td>
<td>5</td>
</tr>
<tr>
<td>TLS</td>
<td>Anonymous</td>
<td></td>
</tr>
</tbody>
</table>

terminal monitor
Use the `terminal monitor` command to enable the display of system messages on the terminal for telnet and SSH sessions.

Syntax
terminal monitor
no terminal monitor
Default Configuration

The default setting is that system messages are not displayed on telnet or SSH sessions. System messages are always displayed on console sessions (serial or out-of-band port connections).

Command Mode

Privileged Exec mode

User Guidelines

Use the `terminal monitor` command enables system messages to be displayed in a Telnet or SSH session.

Use the `no terminal monitor` command to disable the display of system messages on the terminal for Telnet and SSH sessions. Use the `logging monitor` command to display logging messages in a Telnet or SSH session.

Terminal monitor and logging monitor are enabled on console sessions by default.

Example

This example enables the display of system messages and logging messages on the current telnet session.

```
console#terminal monitor
console#configure
console(config)#logging monitor
```
### System and Stack Management Commands

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset-tag</td>
<td>member</td>
<td>show interfaces</td>
<td>show system</td>
</tr>
<tr>
<td>banner exec</td>
<td>memory free low-watermark</td>
<td>show interfaces</td>
<td>show system fan</td>
</tr>
<tr>
<td>banner login</td>
<td>nsf</td>
<td>show interfaces</td>
<td>show system id</td>
</tr>
<tr>
<td>banner motd</td>
<td>ping</td>
<td>show memory cpu</td>
<td>show system power</td>
</tr>
<tr>
<td>banner motd</td>
<td>process cpu</td>
<td>show nsf</td>
<td>show system temperature</td>
</tr>
<tr>
<td>acknowledge</td>
<td>threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>buffers</td>
<td>quit</td>
<td>show power-usage-history</td>
<td>show tech-support</td>
</tr>
<tr>
<td>clear checkpoint</td>
<td>reload</td>
<td>show process app-list</td>
<td>show users</td>
</tr>
<tr>
<td>clear counters</td>
<td>service</td>
<td>show process app-resource-list</td>
<td>show version</td>
</tr>
<tr>
<td>stack-ports</td>
<td>unsupported-transceiver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connect</td>
<td>set description</td>
<td>show process cpu</td>
<td>stack</td>
</tr>
<tr>
<td>cut-through mode</td>
<td>slot</td>
<td>show process proc-list</td>
<td>stack-port</td>
</tr>
<tr>
<td>disconnect</td>
<td>show banner</td>
<td>show router-capability</td>
<td>stack-port shutdown</td>
</tr>
<tr>
<td>exit</td>
<td>show buffers</td>
<td>show sessions</td>
<td>standby</td>
</tr>
<tr>
<td>hardware profile</td>
<td>show checkpoint statistics</td>
<td>show slot</td>
<td>switch renumber</td>
</tr>
<tr>
<td>portmode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>load-interval</td>
<td>show cut-through mode</td>
<td>show supported cardtype</td>
<td>telnet</td>
</tr>
<tr>
<td>locate</td>
<td>show idprom</td>
<td>show supported switchtype</td>
<td>traceroute</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
asset-tag

Use the asset-tag command in Global Configuration mode to specify the switch asset tag. To remove the existing asset tag, use the no form of the command.

Syntax

asset-tag [unit] tag

no asset-tag [unit]

- unit — Switch number. (Range: 1–12)
- tag — The switch asset tag.

Default Configuration

No asset tag is defined by default.

Command Mode

Global Configuration mode

User Guidelines

The asset-tag command accepts any printable characters for a tag name except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may accept entries up to the first illegal character or reject the entry entirely.

Example

The following example specifies the switch asset tag as 1qwepot. Because the unit parameter is not specified, the command defaults to the master switch number.

```plaintext
console(config)# asset-tag 1qwepot
```
**banner exec**

Use the `banner exec` command to set the message that is displayed after a successful login. Use the `no` form of the command to remove the set message.

**Syntax**

`banner exec MESSAGE`

`no banner exec`

- MESSAGE — Quoted text

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration

**User Guidelines**

The exec message may consist of multiple lines. Enter a quote to complete the message and return to configuration mode. Up to 2000 characters may be entered into a banner. Each line entered will consume an extra two characters to account for the carriage return and line feed.

**Example**

```console
console(config)# banner exec "banner text"
```

**banner login**

Use the `banner login` command to set the message that is displayed just before the login prompt after a user has successfully connected to the switch and prior to the login banner. Use `no banner login` command to remove the message.

**Syntax**

`banner login Message`

`no banner login`

- Message — Quoted text
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration

User Guidelines
The login banner can consist of multiple lines. Enter a quote to end the banner text and return to the configuration prompt. Up to 2000 characters may be entered into a banner. Each line entered will consume an extra two characters to account for the carriage return and line feed. Different terminal emulators will exhibit different behaviors when logging in over SSH. See the user guidelines for banner motd acknowledge for some examples.

Example
console(config)# banner login “banner text”

banner motd
Use the banner motd command to set the message that is displayed prior to logging into the switch. Use no banner motd command to remove the message.

Syntax
banner motd MESSAGE
no banner motd
  •  MESSAGE — Quoted text

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration
User Guidelines

The motd banner can consist of multiple lines. Enter a quote to end the banner text and return to the configuration prompt. Up to 2000 characters may be entered into a banner. Each line entered will consume an extra two characters to account for the carriage return and line feed.

The motd banner is usually displayed prior to logging into the switch, although some protocols, for example SSH, may enforce different behavior. See the user guidelines for banner motd acknowledge for some examples.

Example

calendar(config)# banner motd "IMPORTANT: There is a power shutdown at 23:00hrs today, duration 1 hr 30 minutes."

When the MOTD banner is executed, the following displays:

IMPORTANT: There is a power shutdown at 23:00hrs today, duration 1 hr 30 minutes.

banner motd acknowledge

The banner displayed on the console must be acknowledged if banner motd acknowledge is executed. Enter “y” or “n” to continue to the login prompt. If “n” is entered, the session is terminated and no further communication is allowed on that session. However, serial connection will not get terminated if ‘y’ is not entered. Use the no banner motd acknowledge command to disable banner acknowledge.

Syntax

banner motd acknowledge
no banner motd acknowledge

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode
User Guidelines

Various terminal emulators exhibit different behaviors with regards to the MOTD and the acknowledge prompt, for example, TeraTerm and putty. There are also different behaviors based upon the protocol used (SSH versus telnet). See below for some examples where the MOTD prompt occurs either before or after the acknowledge prompt. The banner motd in this example is “If you need to utilize this device or otherwise make changes to the configuration, you may contact Kevin at x911. Please be advised this unit is under test by Kevin.” and the banner login is “Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.”

SSH (putty):

login as: dellradius

If you need to utilize this device or otherwise make changes to the configuration, you may contact Kevin at x911. Please be advised this unit is under test by Kevin.
dellradius@192.168.12.84's password:

Press 'y' to continue (within 30 seconds) (y/n)
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.
N3024-C1>

SSH (Linux Terminal):

[root@kevin ~]# ssh 192.168.12.84 -l dellradius
If you need to utilize this device or otherwise make changes to the configuration, you may contact Kevin at x911. Please be advised this unit is under test by Kevin.
dellradius@192.168.12.84's password:

Press 'y' to continue (within 30 seconds) (y/n)
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.
N3024-C1>

SSH (xterm):
Switch Management Commands

Example

```
console(config)# banner motd "There is a power shutdown at 23:00hrs today, duration 1 hr 30 minutes."
console(config)# banner motd acknowledge
```

When the MOTD banner is executed, the following displays:

IMPORTANT: There is a power shutdown at 23:00hrs today, duration 1 hr 30 minutes. Press 'y' to continue

If ‘y’ is entered, the following displays:

```
console>
```

If ‘n’ is entered, the session will get disconnected, unless it is a serial connection.

buffers

Use the `buffers` command to configure the rising and falling thresholds for the issuance of the message buffer SNMP trap and notification via a SYSLOG message.
Syntax

buffers {rising-threshold rising-threshold-val | falling-threshold falling-threshold-val | severity severity-level}

no buffers {rising-threshold | falling-threshold | severity }

- rising-threshold-val—The rising message buffer threshold over which a trap will be issued. This is a percentage of messages buffers utilized and ranges from 0 to 100.
- falling-threshold-val—The falling threshold value. Once the rising threshold has been crossed, another trap will not be issued until the message buffer has dropped below the falling threshold. This is a percentage of messages buffers utilized and ranges from 0 to 100.
- severity-level—The severity level of the trap issued by SNMP. Range is 0 (EMERGENCY) to 7 (DEBUG).

Default Configuration

The default rising-threshold-val is 80%.
The default falling-threshold-val is 50%
The default severity level is NOTICE.

Command Mode

Global Configuration

User Guidelines

Message buffers are used internally by the switch firmware to pass network PDUs. This includes PDUs such as spanning tree BPDUs or multicast or unicast packets forwarded in software. On rare occasions, a packet storm may cause the switch to become congested due to an excessive number of messages forwarded to the switch CPU. The switch has numerous rate limiters and other mechanisms to appropriately handle such packet floods, however, due to the changing nature of Internet traffic, new types of traffic may cause temporary internal congestion conditions. This command allows the operator to enable the issuance of a trap in such a condition as an aid to early diagnosis and mitigation of the conditions causing traffic to flood the switch CPU.

Setting the rising threshold to 0 disables message buffer monitoring.
The falling-threshold-val should be configured to be less than or equal to the rising-threshold-val.

**Command History**
Introduced in version 6.2.0.1 firmware.

**Example**
```
console(config)#buffers rising-threshold 90
```

### clear checkpoint statistics

Use the `clear checkpoint statistics` command to clear the statistics for the checkpointing process.

**Syntax**
clear checkpoint statistics

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode

**User Guidelines**
When nonstop forwarding is enabled on a stack, the stack's management unit checkpoints operational data to the backup unit. If the backup unit takes over as the management unit, the control plane on the new management unit uses the checkpoint data when initializing its state. Checkpoint statistics track the amount of data checkpointed from the management unit to the backup unit.

**Example**
```
console#clear checkpoint statistics
```

### clear counters stack-ports

Use the `clear counters stack-ports` command to clear the statistics for all stack-ports.
Switch Management Commands

Syntax

clear counters stack-ports

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

This command resets all statistics shown by the show switch stack-ports counters and the show switch stack-ports diag commands.

Example

console#clear counters stack-ports

connect

Use this command to connect the serial console of a different stack member to the local unit. The connect command allows administrations that deploy terminal servers to connect a single serial line to any stack member for administration of the stack via the console. The network administrator can use the connect command to access the master unit console session when presented with a “CLI unavailable message” due to a master switchover.

Syntax

connect unit

- unit—A unit number in the stack.

Default Configuration

There is no default configuration for this command.

Command Modes

Privileged Exec mode on stack master.

Unit Prompt on stack member.
**User Guidelines**

This command is available from the Unit prompt on a member unit serial port. The user need not be currently connected over the serial port to connect to another unit.

The stack member being connected to must be up and running and connected as part of the stack. This command connects the the serial console from the target stack member to the local unit. There is only one console session allowed per stack. The remote console session is not restarted and the privilege level is not changed as a result of being connected to the local unit. All security mechanisms applicable to the serial port remain in place.

**Example**

Example 1:
To connect to a remote stack member from master.

```
Stack-Master#connect 2
Remote session started. Type "exit" to exit the session.
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>
```

Example 2:
To connect to the stack master (unit 1, below) over a stack member serial port.

```
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#
```

**cut-through mode**

Use the *cut-through mode* command to enable the cut-through mode on the switch. The mode takes effect on all ports on next reload of the switch. To disable the cut-through mode on the switch, use the no form of this command.

**Syntax**

```
cut-through mode
```
no cut-through mode

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration

**User Guidelines**
Cut-through mode is only supported on Dell EMC Networking N4000 series switches. It is not supported on Dell EMC Networking N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON Series switches.

**Example**
```
console(config)#cut-through mode
The mode (enable) is effective from the next reload of Switch/Stack.
```

disconnect
Use the disconnect command to detach a UI session.

**Syntax**
disconnect { session-id | all }

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode.

**User Guidelines**
This command forcibly logs out and disconnects a Telnet, SSH, HTTP or HTTPs session. Use the show sessions command to display the session identifier.

The session identifier ranges from 0-42. The all parameter disconnects all telnet, SSH, HTTP or HTTPs sessions.
It is not possible to disconnect the EIA-232 (serial console) session.

**exit**

Use this command to disconnect the serial connection to a remote unit.

**Syntax**

exit

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

User Exec mode on stack master.

Unit prompt on the stack member.

**User Guidelines**

This command is available in User Exec mode on the master unit serial port and from the Unit prompt on member unit serial ports. The user need not be currently connected over the serial port to connect to another unit.

The stack member being connected to must be up and running and connected as part of the stack.

**Example**

Example 1:

To disconnect a remote session to a stack member established from the stack manager.

Stack-Master#connect 2

Remote session started. Type "exit" to exit the session.

(Interval 2 - CLI unavailable - please connect to master on Unit 1)>exit

Stack-Master#
To disconnect a remote session to the stack master established from a stack member.

(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 2

(Unit 2 - CLI unavailable - please connect to master on Unit 1)>
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#
Stack-Master#exit

Stack-Master>exit

(Unit 2 - CLI unavailable - please connect to master on Unit 1)>

**hardware profile portmode**

Use the **hardware profile portmode** command in Interface Configuration mode to configure a 40G port in 4x10G mode or 1x40G mode.

Use the no form of the command to return the port to the default mode (1x40G).

**Syntax**

```
hardware profile portmode {1x40g|4x10g}
no hardware profile portmode
```

- **1x40g**—Configure the port as a single 40G port using 4 lanes.
- **4x10g**—Configure the port as four 10G ports, each on a separate lane. This mode requires the use of a suitable 4x10G to 1x40g pigtail cable.

**Default Configuration**

By default, 40G ports are configured in 1x40G mode.

**Command Mode**

Interface Configuration mode

**User Guidelines**

This command is only available on the N4000 series switches. This command can only be executed on the 40G interface. Entering this command on any of the 4x10G interfaces (or any other 10G port) will give an error.
This command takes effect only after rebooting the switch.

**hostname**

Use the `hostname` command in Global Configuration mode to specify or modify the switch host name. To restore the default host name, use the `no` form of the command.

**Syntax**

```
hostname name
no hostname
```

- **name** — The name of the host. (Range: 1–255 characters) The command allows spaces in the host name when specified in double quotes. For example, `#snmp-server v3-host “host name”`.

**Default Configuration**

No host name is configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

The hostname, if configured, is advertised in the LLDP system-name TLV. The hostname may include any printable characters except a question mark. Enclose the string in double quotes to include spaces within the name. The surrounding quotes are not used as part of the name. The CLI does not filter illegal characters and may truncate entries at the first illegal character or reject the entry entirely.

**Example**

The following example specifies the switch host name.

```text
console(config)# hostname Dell
```
**initiate failover**

To manually force a failover from the management unit to the backup unit in a stack, use the `initiate failover` command in Stack Configuration mode.

The `initiate failover` command checks for stack port errors and NSF synchronization prior to initiating failover. If stack port errors are found, or if the NSF status is not synchronized, a message is displayed and the user is prompted to continue or abort the operation (see example, below).

**Syntax**

`initiate failover`

**Default Configuration**

There is no default configuration.

**Command Mode**

Stack Configuration mode

**User Guidelines**

This command forces a warm restart of the stack. The backup unit takes over as the new management unit without clearing the hardware state on any of the stack members. The original management unit reboots. If the system is not ready for a warm restart, for example because no backup unit has been elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message. Use the `standby` command to select a specific unit to act as the backup unit. Use the `show nsf` command to check the NSF state. If the switch shows Warm Restart Ready as Yes, then the master switch state is synchronized with the standby switch.

**Examples**

**Example-No Stack Port Errors**

```
console(config-stack)#initiate failover  ?
<cr> Press enter to execute the command.
console(config-stack)#initiate failover
Management unit will be reloaded.
Are you sure you want to failover to the backup unit? (y/n) y
```
Example-Stack Port Errors

console(config-stack)#initiate failover
Warning! Stack errors detected on the following interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Error Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>12</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>22</td>
</tr>
</tbody>
</table>

NSF Status: Not synchronized

Stack port errors or lack of NSF synchronization may indicate a non-redundant stack topology exists. Fail-over on a non-redundant topology may cause the stack to split!

Management unit will be reloaded. Are you sure you want to failover to the backup unit? (y/n)

load-interval

Use this command to load the interface utilization measurement interval. Use the no form of this command to reset the duration to the factory default value.

Syntax

load-interval time

no load-interval

  time—The number of seconds after which interface utilization is measured periodically. The time has to be a multiple of 30. (Range 30-600 seconds)

Default Configuration

The default interval is 300 seconds.

Command Modes

Interface Configuration mode, Interface Range Configuration mode, Port Channel Configuration mode, Port Channel Range Configuration mode.
User Guidelines
This command has no user guidelines.

Example
console(config-if-Gi1/0/1)#load-interval 150

locate
Use the locate command to locate a switch by LED blinking.

Syntax
locate [switch unit] [time time]
• switch unit—If multiple devices are stacked, you can choose which switch to identify.
• time time —LED blinking duration in seconds. Range 1-3600 seconds.

Default Configuration
Default value is 20 seconds.

Command Mode
Privileged Exec

User Guidelines
When this command is executed on N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON switches, the front panel power supply 1 LED blinks. On N4000 switches, the back panel green Locator LED blinks.
The LED blinks until it times out. The user may select a new time value while the LED is blinking. The last value selected takes effect immediately. The locate command does not persist across reboots.

Example
console# locate switch 1 time 555
logout

Use this command to disconnect the serial connection to the remote unit on the stack member.

Syntax
logout

Default Configuration
There is no default configuration for this command.

Command Modes
User Exec mode on the stack master. Unit prompt on the stack member.

User Guidelines
This command is available in User Exec mode on the master unit serial port and from the Unit prompt on member unit serial ports. The user need not be currently connected over the serial port to connect to another unit.
The stack member being connected to must be up and running and connected as part of the stack.
This command is an alias for the exit command.

Example
(Example 1:
To disconnect a remote session to stack master established from a stack member.
Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#
Stack-Master#logout
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>

Example 2:
To disconnect a remote session to stack master established from a stack member.
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#exit
Stack-Master>logout
member

Use the member command in Stack Configuration mode to preconfigure a switch stack member. Execute this command on the Management Switch. To remove a stack-member configuration from the stack, use the no form of the command.

⚠️ The no form of the command may not be used if the member is present in the stack.

Syntax

member unit switchindex

no member unit

• unit — The switch identifier of the switch to be added or removed from the stack. (Range: 1–12)
• switchindex — The index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is obtained from the show supported switchtype command.

Default configuration

This command has no defaults.

Command Mode

Stack Configuration

User Guidelines

The switch index (SID) can be obtained by executing the show supported switchtype command in User Exec mode. When removing a unit from a stack, use the no member command to remove the stack member configuration after physically removing the unit.

Example

The following example displays how to add to stack switch number 2 with index 1.

console(config)# stack
console(config-stack)# member 2 1
**memory free low-watermark**

Use the `memory free low-watermark` command to configure the notification of a low memory condition on the switch. for the issuance of the CPU overload SNMP trap and notification via a SYSLOG message. Use the `no` form of the command to return the threshold to its default value.

**Syntax**

```
memory free low-watermark processor [kb]
no memory free low-watermark processor
```

- `kb`—The amount of free memory (in Kilobytes) below which a trap is issued and a message is logged.

**Default Configuration**

The default low memory notification is 0 MB.
The SYSLOG notification message is issued with severity NOTICE.

**Command Mode**

Global Configuration

**User Guidelines**

Use the `show memory cpu` command to display the allocated and free memory.

Setting the threshold to 0 disables low memory notifications.
The traps and SYSLOG messages are suppressed if they occur more frequently than once a minute.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

This example sets the notification for low memory at 1 megabyte. A notice message and trap will be issued if free memory falls below 1M and another notice message and trap will be issued when free memory rises above 1M.

```
console(config)#memory free low-watermark processor 1000
```
**nsf**

Use this command to enable non-stop forwarding. The `no` form of the command will disable NSF.

**Syntax**

nsf
no nsf

**Default Configuration**

Non-stop forwarding is enabled by default.

**Command Mode**

Stack Configuration mode

**User Guidelines**

Nonstop forwarding allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack management unit.

**Example**

```
console(config)#nsf
```

**ping**

Use the `ping` command to check the accessibility of the specified station on the network.

Use of the optional VRF parameter executes the command within the context of the VRF specific routing table.
Syntax

```
ping [vrf vrf-name] [ [ ip ] ip-address | hostname | { ipv6 { interface interface-id | vlan vlan-id | loopback loopback-id | out-of-band | tunnel tunnel-id} link-local-address | ipv6-address | hostname} [ count count] [ interval interval] [ size size] [ source { ip-address | ipv6-address | interface-id | vlan vlan-id | out-of-band}] ]
```

- `ip-address`—The IPv4 address to ping.
- `ipv6-address`—The IPv6 address to ping.
- `link-local-address`—The link local IPv6 address to ping.
- `hostname`—The domain name of the host to ping. (Range: 1–158 characters). When used with the IPv6 keyword, the hostname will be resolved to an IPv6 address, otherwise, it will be resolved to an IPv4 address.
- `vrf-name`—(Optional) The name of the VRF instance from which to ping. Only hosts reachable from within the VRF instance can be pinged. If a source parameter is specified in conjunction with a VRF parameter, it must be a member of the VRF. The `ipv6` parameter cannot be used with the `vrf` parameter.
- `interface-id`—The interface over which a link local IPv6 address may be reached. Only available when used with the IPv6 keyword.
- `repeat`—The number of ping packets to send. (Range: 1–100 packets).
- `interval`—The time between Echo Requests, in seconds (Range: 1–60 seconds).
- `size`—Number of data bytes in a packet (Range: 0–13000 bytes).
- `source ip-address`—The ping packets are transmitted using the specified source IP address.
- `source loopback loopback-id`—The ping packets are transmitted with the source address of the loopback interface.
- `source vlan vlan-id`—The ping packets are transmitted over the VLAN with the source address of the VLAN.
- `source tunnel tunnel-id`—The ping packets are transmitted with the source address of the tunnel.
- `out-of-band`—The ping packets are transmitted over the out-of-band interface.
**Default Configuration**

The default mode is IPv4. The command defaults to an IPv4 address.
The default ping count is 4.
The default interval is 1 second.
The default packet size is 0 data bytes.
The packet size is specified in bytes and refers to the packet payload, not the frame size.
Packets are padded to extend the frame to the minimum legal frame length by default.

**Command Mode**

User Exec mode, Privileged Exec mode

**User Guidelines**

If the ipv6 or ip parameter is specified, all the other arguments must match (i.e., it is not possible to ping an IPv6 address from an IPv4 source and vice-versa).

The ipv6 parameter must be specified if an IPv6 address is entered. Otherwise, the command will interpret the IPv6 address as a hostname parameter.

The switch can be pinged from a remote IPv4/IPv6 host with which the switch is connected through the default VLAN (VLAN 1) or another VLAN, if configured, as long as there is a physical path between the switch and the host.

Use the optional interface keyword to ping an IPv6 link-local interface by using the IPv6 link-local address or the global IPv6 address of the interface as the destination address in the ICMP echo packet.

Use the source keyword to specify the source IPv6 address to use in the ping packet and to specify the source interface on which to transmit the ICMP packet. The source can be a loopback, tunnel, logical interface, or the out-of-band interface.
If a host name is specified, a DNS server must be configured locally on the switch and the host name must resolve to an IPv4/IPv6 address as appropriate for the syntax entered. The command allows spaces in the host name when specified in double quotes, even though host names may only consist of letters, numbers and the hyphen character.

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the vrf parameter.

The vrf parameter is only available on the N3000/N3100/N4000 switches. Loopback interfaces are not supported on the N1100-ON Series switches.

**Examples**

The following example sends an IPv4 ICMP Echo request from VLAN 3 to 10.1.1.3

```
console#ping 10.1.1.3 source vlan 3
```

The following example determines whether the loopback interface is reachable on the network at the IPv6 address specified.

```
console(config)#ping ipv6 interface loopback 1 FE80::202:BCFF:FE00:3068
```

Pinging fe80::21e:c9ff:fede:b137 with 0 bytes of data:

Reply From fe80::21e:c9ff:fede:b137: icmp_seq = 0. time <10 msec.
Reply From fe80::21e:c9ff:fede:b137: icmp_seq = 1. time <10 msec.
Reply From fe80::21e:c9ff:fede:b137: icmp_seq = 2. time <10 msec.
Reply From fe80::21e:c9ff:fede:b137: icmp_seq = 3. time <10 msec.

The following example determines whether another computer is reachable over the network at the IPv6 address specified.

```
console#ping ipv6 2030:1::1
```

Pinging 2030:1::1 with 0 bytes of data:

Reply From 2030:1::1: icmp_seq = 0. time <10 msec.
Reply From 2030:1::1: icmp_seq = 1. time <10 msec.
Reply From 2030:1::1: icmp_seq = 2. time <10 msec.
Reply From 2030:1::1: icmp_seq = 3. time <10 msec.
process cpu threshold

Use the process cpu threshold command to configure the rising and falling thresholds for the issuance of the CPU overload SNMP trap and notification via a SYSLOG message. Use the no form of the command to return the thresholds to their default values.

Syntax

process cpu threshold type total  rising percentage interval seconds [ falling percentage interval seconds ]

no process cpu threshold total type {rising | falling }

- **rising** percentage—The rising CPU percentage threshold over which a trap will be issued and a message logged. This is a percentage of CPU utilized over the period and ranges from 1 to 100.
- **falling** percentage—The falling threshold value under which a trap will be issued and message logged. This is a percentage of CPU utilized and ranges from 1 to 100.
- **interval** seconds—The number of seconds in the exponential weighted moving average period (multiple of 5 seconds).

Default Configuration

- The default rising-threshold-val is 0%.
- The default falling-threshold-val is 0%.
- The default interval is 0 seconds.
- The default severity level is NOTICE.

Command Modes

Global Configuration

User Guidelines

CPU utilization is calculated using Exponential Moving Weighted Average (EMWA) over the total time period. The EMWA is calculated using the following formula:

\[ \text{EMWA(current\_period)} = \text{EMA(prev\_period)} + (\text{currentUtilization} - \text{EMA(prev\_period)}) \times \text{weight} \]
where weight = 2 / ((TotalTimePeriod/samplePeriod) + 1). The sample period is 5 seconds. The utilization monitoring time period can be configured from 5 secs to 86400 seconds in multiples of 5 seconds.

Setting a threshold or interval to 0 disables that individual function.

The falling-threshold percentage should be configured to be less than or equal to the rising-threshold percentage. The switch reports the task level CPU utilization for the last 5 second, 1 minute and 5 minute periods. To aid the operator in troubleshooting when the CPU utilization has crossed the rising threshold, the show proc cpu command has been extended to show the task/total CPU utilization for the rising threshold period also. If the utilization thresholds are not configured, then the utilization for last 5 secs, 1 minute and 5 minutes is displayed as before. The CPU utilization for any given period is displayed in only after the first average has been calculated over the time period.

For instance, the 5 minute average is shown only after the switch has been up for more than 5 minutes. Additionally, whenever a time-period is configured for CPU utilization monitoring, the existing utilization data for the time-period is cleared and average is built again over the time period. This is done to prevent generation of notifications based on the old utilization data.

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```console
console(config)#process cpu threshold type total rising 90 interval 100
```

**quit**

Use this command to disconnect the serial connection to the remote unit on the stack member.

**Syntax**

```console
quit
```

**Default Configuration**

There is no default configuration for this command.
**Command Modes**
User Exec mode on the stack master. Unit prompt on the stack member.

**User Guidelines**
This command is available in User Exec mode on the master unit serial port and from the Unit prompt on member unit serial ports. The user need not be currently connected over the serial port to connect to another unit.
The stack member being connected to must be up and running and connected as part of the stack.
This command is an alias for the `exit` command.

**Example**
Example 1:
To disconnect a remote session to the stack master established from a stack member.

(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#
Stack-Master#quit
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>

Example 2:
To disconnect a remote session to the stack master established from stack member.

(Unit 2 - CLI unavailable - please connect to master on Unit 1)>connect 1
Stack-Master#exit
Stack-Master>quit
(Unit 2 - CLI unavailable - please connect to master on Unit 1)>

**reload**
Use the `reload` command to reload stack members.

The reload command checks for stack port errors prior to reloading stack members and after the check for unsaved configuration changes. If stack port errors are found, a message is displayed.

**Syntax**
`reload [stack-member-number]`
• stack–member–number—The stack member to be reloaded.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Priveleged Exec mode

**User Guidelines**
If no unit is specified, all units in a stack are reloaded. When copying firmware onto the switch in a stacked configuration, use the `show sfs` and `show version` commands to check the status of stack firmware synchronization prior to a reboot.

**Examples**

**Example-Reloading the Stack**
The following example displays how to reload the stack.

```
console#reload 1
Management switch has unsaved changes.
Would you like to save them now? (y/n)n
Configuration Not Saved!
Are you sure you want to reload the switch? (y/n) y
Reloading management switch 1.
```

**Example-Stack Port Errors**
The following example shows stack port errors detected by the command.

```
console#reload
Management switch has unsaved changes.
Are you sure you want to continue? (y/n)

Warning! Stack port errors detected on the following interfaces:
Interface         Error Count
----------------  ----------------
Gi1/0/1           12
Gi1/0/3           22

Stack port errors may indicate a non-redundant stack topology exists. Failover on a non-redundant topology may cause the stack to split!
```
Are you sure you want to reload the stack? (y/n)

**service unsupported-transceiver**

Use this command to avoid the following on using an unsupported optic.

- Logging of a message.
- Generation of SNMP trap.

Use the `no` form of this command to set the transceiver support to the factory default.

**Syntax**

```
service unsupported-transceiver
no service unsupported-transceiver
```

**Default Configuration**

The default configuration is to log a message along with the SNMP trap generation on insertion or removal of an optic that is not qualified by Dell.

**Command Mode**

Global Configuration mode

**User Guidelines**

The switch logs a message and generates a trap on inserting or removing an optics not qualified by Dell. This command suppresses the above mentioned behavior.

**Example**

The following example bypasses logging of a message and trap generation on inserting or removing an optics not qualified by Dell.

```
console(config)# service unsupported-transceiver
```

**set description**

Use the `set description` command in Stack Configuration mode to associate a text description with a switch in the stack.
**Syntax**

```
set description unit description
```

- **unit** — The switch identifier. (Range: 1–12)
- **description** — The text description. (Range: 1–80 alphanumeric characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Stack Configuration mode

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays

```
console(config)#stack
cfg(config-stack)#set description 1 "unit 1"
```

**slot**

Use the `slot` command to configure a slot in the system. The unit/slot is the slot identifier of the slot located in the specified unit. The card index is the index to the database of the supported card types (see the command `show supported cardtype`) indicating the type of card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be reconfigured with default information for the card. The supported card types are:

- Dell EMC Networking N2024
- Dell EMC Networking N2024P
- Dell EMC Networking N2048
- Dell EMC Networking N2048P
- Dell EMC Networking N3024
Use the `no` form of the command to return the unit/slot configuration to the default value.

**Syntax**

`slot` unit/slot cardindex

`no slot` unit/slot

- unit/slot — The slot identifier of the slot.
- cardindex — The index into the database of the supported card types (see `show supported cardtype`) indicating the type of card being preconfigured in the specified slot. The card index is a 32-bit integer.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration

**User Guidelines**

The card index (CID) can be obtained by executing the `show supported cardtype` command.

Administrators may issue multiple consecutive slot commands addressing a particular unit/slot without issuing an intervening `no` slot command.
**Example**

```
console(config)#slot 1/3 3
console(config)#slot 1/3 4
```

**show banner**

Use the `show banner` command to display banner information.

**Syntax**

```
show banner
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console#show banner

Banner: Exec
Line Console...................... Enable
Line SSH.......................... Disable
Line Telnet....................... Enable
=== exec ===

Banner: Login
Line Console...................... Enable
Line SSH.......................... Enable
Line Telnet....................... Disable
=== login ===

Banner: MOTD
Line Console...................... Enable
Line SSH.......................... Enable
Line Telnet....................... Enable
=== motd ===
```
**show buffers**

Use the `show buffers` command to display the system allocated buffers.

**Syntax**

```
show buffers
```

**Default Configuration**

There is no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The internal message buffers are partitioned into one transmit group reserved for system generated messages and five receive priority groups. The receive priority groups are processed in strict priority order starting with the High group and proceeding down through the Mid0, Mid1 and Mid2 groups down to the Normal group. Small numbers of buffer failures in the low priority groups (Norm, Mid2, Mid1) may occur without affecting system operation, (for example, loss of an LLDP packet is not likely to cause any noticeable system disruption).

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console#show buffers

Message Buffer Utilization
----------------------------
0 of 246 total buffers used

<table>
<thead>
<tr>
<th>Receive</th>
<th>Attempts</th>
<th>Failures</th>
<th>%Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norm</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Mid2</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>
```
show checkpoint statistics

Use the `show checkpoint statistics` command to display the statistics for the checkpointing process.

**Syntax**

`show checkpoint statistics`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

When nonstop forwarding is enabled on a stack, the stack's management unit checkpoints operational data to the backup unit. If the backup unit takes over as the management unit, the control plane on the new management unit uses the checkpointed data when initializing its state. Checkpoint statistics track the amount of data checkpointed from the management unit to the backup unit.

**Example**

```
console#show checkpoint statistics
```
show cut-through mode

Use the `show cut-through mode` command to show the cut-through mode on the switch.

**Syntax**

`show cut-through mode`

**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**Default Configuration**

This command has no default configuration.

**User Guidelines**

This command is not available on N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON switches.

**Example**

```
Console#show cut-through mode
Current mode    : Enable
Configured mode : Disable (This mode is effective on next reload)
```

show hardware profile

Use the `show hardware profile` command to display the hardware profile information for the 40G ports. The user can optionally specify an interface or all 40G interfaces are displayed.
**Syntax**

```
show hardware profile portmode [interface-id]
```

**Default Configuration**

This command has no default setting.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command is not available on the N1100-ON/N1500/N2000/N2100-ON/N3000/N3100-ON switches.

**Examples**

```
console#show hardware profile portmode
Configured  Running
-------------  --------------  ----------  -------
40G Interface  10G Interfaces  Mode        Mode
-------------  --------------  ----------  -------
Fo1/0/1        Te1/0/25-28     1x40G       4x10G
Fo1/0/2        Te1/0/29-32     1x40G       1x40G
```

```
console#show hardware profile portmode fo1/0/1
Configured  Running
-------------  --------------  ----------  -------
40G Interface  10G Interfaces  Mode        Mode
-------------  --------------  ----------  -------
Fo1/0/1        Te1/0/25-28     1x40G       4x10G
```

**show idprom interface**

Use this command to display the optics EEPROM contents in user-readable format.

**Syntax**

```
show idprom interface interface-id
```

- `interface-id`—The Ethernet interface.
**Default Configuration**
This command has no default configuration.

**Command Modes**
User Exec, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command has no user guidelines.

**Example**
The following example shows the optic parameters in user readable format.

```
console#show idprom interface tengigabitethernet 1/0/9
```

- Type.............................. SFP+
- Media............................. 10GBASE-LRM
- Serial Number..................... ANF0L5J
- Dell EMC Qualified................ Yes

The following example shows the optic parameters, but not the IDPROM content as the entered activation code in incorrect.

```
console#show idprom interface tengigabitethernet 1/0/9 debug abc
```

- Type.............................. SFP+
- Media............................. 10GBASE-LRM
- Serial Number..................... ANF0L5J
- Dell EMC Qualified................ Yes

**show interfaces**
Use the `show interfaces` command to display the traffic statistics for one or multiple interfaces. If no parameter is given, all interfaces are shown.

**Syntax**
```
show interfaces interface-id
```

- **interface-id**—The ID for any valid Ethernet interface (that is, a 1G, 10G, or 40G interface in standard interface format or a port-channel identifier).
**Default Configuration**

This command has no default configuration.

**Command Modes**

All modes

**User Guidelines**

The `show interface` command shows the actual operational status of the interface, which is not necessarily the same as the configuration.

Input/output rate statistics are collected every 10 seconds.

The RX and TX utilization (sum of the individual active links) is shown for port-channels. The utilization is measured in kilobits per second.

**Command History**

Updated examples and guidelines in version 6.5 firmware.

**Example**

The following example shows the output for a 1G interface:

```
console#show interfaces gi1/0/1

Interface Name : .............................. Gi1/0/1
SOC Hardware Info : ............................. BCM56342_A0
Link Status : .................................. Up
Keepalive Enabled.............................. True
Err-disable Cause.............................. None
VLAN Membership Mode: ......................... Trunk Mode
VLAN Membership: .............................. (1),2-3,101-113,813,3232
MTU Size : .................................... 1518
Port Mode [Duplex] : ............................. Full
Port Speed : ................................... 1000
Link Debounce Flaps : ........................... 0
Auto-Negotiation Status : ........................ Auto
Burned MAC Address : ........................... 001E.C9DE.B110
L3 MAC Address................................. 001E.C9DE.B112
Sample load interval : ........................... 300
Received Input Rate Bits/Sec : ................. 784
Received Input Rate Packets/Sec : ............... 1
Transmitted Input Rate Bits/Sec : ............... 1344
Transmitted Input Rate Packets/Sec : ............ 1
```
Total Packets Received Without Errors.......... 102792
Unicast Packets Received.......................... 0
Multicast Packets Received......................... 102792
Broadcast Packets Received........................ 0
Total Packets Received with MAC Errors......... 0
Jabbers Received.................................. 0
Fragments/Undersize Received-------------------- 0
Alignment Errors.................................. 0
FCS Errors........................................ 0
Overruns............................................ 0
Total Received Packets Not Forwarded............. 7
Total Packets Transmitted Successfully......... 147070
Unicast Packets Transmitted....................... 0
Multicast Packets Transmitted..................... 147070
Broadcast Packets Transmitted.................... 0
Transmit Packets Discarded....................... 0
Total Transmit Errors............................. 0
Total Transmit Packets Discarded.................. 0
Single Collision Frames........................... 0
Multiple Collision Frames.......................... 0
Excessive Collision Frames......................... 0

console#show interfaces po1
Intf Ports                    Ch-Type  Hash Min-link Local Prf TX Util RX Util
---- ------------------------ -------- ---- -------- --------- ------- -----
--
Po1  Active: Te1/0/1, Te1/0/2 Dynamic  7    1        Disabled   432344   83782

Utilization is shown in Kbps.

Hash Algorithm Type
1 - Source MAC, VLAN, EtherType, source module and port Id
2 - Destination MAC, VLAN, EtherType, source module and port Id
3 - Source IP and source TCP/UDP port
4 - Destination IP and destination TCP/UDP port
5 - Source/Destination MAC, VLAN, EtherType, source MODID/port
6 - Source/Destination IP and source/destination TCP/UDP port
7 - Enhanced hashing mode

show interfaces advanced firmware

Use the show interfaces advanced firmware command to display the firmware revision of the PHY for a port with upgradable firmware.
Switch Management Commands

Syntax
show interfaces advanced firmware interface
  •  interface—A firmware upgradable Ethernet interface.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command is only applicable to firmware upgradable interfaces. 1G interfaces are never shown in the command output. Some 10G interfaces may show as not firmware upgradable.

Example
console#show interfaces advanced firmware
Port  Revision  Part number
------- -------- ------------
Te1/0/1 0x411  BCM8727
Te1/0/2 0x411  BCM8727
Te1/0/3 0x411  BCM8727
Te1/0/4 0x411  BCM8727
Te1/0/5 0x411  BCM8727

show interfaces utilization
Use this command to display interface utilization.

Syntax
show interfaces utilization [interface-id]
  •  interface-id—A Ethernet or port-channel interface identifier.

Default Configuration
There is no default configuration for this command.
**Command Modes**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
This command displays interface transmit and receive utilization in bits/sec and packets/sec. The transmit utilization and transmit packet counts include packets generated by the CPU.

Buffer utilization is the count of cells queued for transmission on a port. A buffer utilization value of less than 10 generally indicates that the port is not experiencing congestion and packets are transmitted as soon as they are queued for output. A value above 10 that increases and decreases indicates a port that is experiencing burstiness. A persistent value above 10 indicates a port that is experiencing congestion (incast); if the cell count continues to increase over time, the port begins discarding packets when reaching the tail drop threshold.

The value of 10 cells above corresponds to one and one-half maximum length packets queued for transmission. For the N1100-ON, N2000, N2100-ON, N3000, N3100-ON, and N4000 switches, the cell size is 208 bytes; for the N1500, the cell size is 128 bytes. If jumbo frames are enabled (MTU 9200), the expected size of a single maximum length packet is 45 cells (9200/208 = 44.2). Allowing for a frame and a half to be buffered on average, a value of 75 is perhaps more appropriate to consider as the indicator for determining if congestion exists on a port.

The clear counters command clears the underlying counters for transmit and receive utilization values, transmit and receive packets per second values, and the drops counter. The count of buffered packets is not a sampled counter and cannot be cleared.

This command displays the following interface transmit and receive utilization in bits/sec and packets/sec.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface for which information is displayed.</td>
</tr>
<tr>
<td>Load Interval</td>
<td>The load interval for the interface.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper. Speed</td>
<td>The operational speed, which is the speed at which the interface is currently operating (e.g., 1M, 10M, 100M, 1G, 10G, 40G).</td>
</tr>
<tr>
<td>Rx Util</td>
<td>The receive utilization which is the link utilization in the receive direction as a percentage of operational speed (range 0-100). The utilization is derived by dividing the link speed by the number of bytes received averaged over the last sampling interval.</td>
</tr>
<tr>
<td>Tx Util</td>
<td>The transmit utilization. The link utilization in the transmit direction as a percentage of operational speed (range 0-100). The utilization is derived by dividing the link speed by the number of bytes received averaged over the last sampling interval.</td>
</tr>
<tr>
<td>Rx PPS</td>
<td>The received packets per second. This value is the average number of packets received over the last sampling interval.</td>
</tr>
<tr>
<td>Tx PPS</td>
<td>The transmitted packets per second. This value is the average number of packets transmitted over the last sampling interval.</td>
</tr>
<tr>
<td>Buffer Size</td>
<td>The number of bytes queued for egress on the interface. This value is calculated as the number of cells multiplied by the cell size (cell size is hardware specific) and is read directly from the hardware, i.e. this value is not sampled.</td>
</tr>
<tr>
<td>Drop Count</td>
<td>The number of packets queued for egress that are dropped for any reason. It is the same value as shown for “Transmit Packets Discarded” in the show statistics command.</td>
</tr>
</tbody>
</table>
Example

The following example shows a classical incast situation on interface Gi1/0/2 where the port is fully utilized or nearly fully utilized, buffering many frames (with increased latency) and beginning to drop frames as the internal thresholds for buffering on the port are reached. A conscientious network operator might want to examine why the devices attached to Gi1/0/5 and Gi1/0/6 are sending so much traffic to Gi1/0/2 attached devices and either re-distribute the devices, rate-limit traffic egressing the devices attached to Gi1/0/5 and Gi1/0/6, or increase the number of links available for the device attached to Gi1/0/2.

```
console#show interfaces utilization

<table>
<thead>
<tr>
<th>Port</th>
<th>Load Interval Speed</th>
<th>Oper. Util</th>
<th>Rx PPS</th>
<th>Tx PPS</th>
<th>Rx Buffer Size</th>
<th>Tx Buffer Size</th>
<th>Drop Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>300</td>
<td>10M</td>
<td>1</td>
<td>0</td>
<td>296</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>300</td>
<td>1G</td>
<td>99</td>
<td>0</td>
<td>674500</td>
<td>938098</td>
<td>1102</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>300</td>
<td>1G</td>
<td>0</td>
<td>15</td>
<td>0</td>
<td>112428</td>
<td>7</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>300</td>
<td>1G</td>
<td>37</td>
<td>0</td>
<td>249565</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>300</td>
<td>1G</td>
<td>88</td>
<td>1</td>
<td>593560</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

show memory cpu

Use the `show memory cpu` command to check the total and available RAM space on the switch.

Syntax

```
show memory cpu
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**
No specific guidelines.

**Example**

```
console#show memory cpu
```

Total Memory......................... 262144 KBytes
Available Memory Space............... 121181 KBytes

**show nsf**

Use the `show nsf` command to show the status of non-stop forwarding.

**Syntax**

```
show nsf
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The Global Status Parameters for NSF are explained as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF Administrative Status</td>
<td>Whether nonstop forwarding is administratively enabled or disabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>NSF Operational Status</td>
<td>Indicates whether NSF is enabled on the stack.</td>
<td>Enabled</td>
<td>None</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Range</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Last Startup Reason</td>
<td>The type of activation that caused the software to start the last time. There are four options. “Power-On” means that the switch rebooted. This could have been caused by a power cycle or an administrative “Reload” command. “Administrative Move” means that the administrator issued a command for the stand-by manager to take over. “Warm-Auto-Restart” means that the primary management card restarted due to a failure, and the system executed a nonstop forwarding failover. “Cold-Auto-Restart” means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.</td>
<td>Power-On</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrative-Move</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warm-Auto-Restart</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cold-Auto-Restart</td>
<td></td>
</tr>
<tr>
<td>Time Since Last Restart</td>
<td>Time since the current management card became the active management card. For the backup manager, the value is set to 0d 00:00:00</td>
<td>Time Stamp</td>
<td>0d 00:00:00</td>
</tr>
<tr>
<td>Restart in progress</td>
<td>Whether a restart is in progress. A restart is not considered complete until all hardware tables have been fully reconciled.</td>
<td>Yes or No</td>
<td></td>
</tr>
<tr>
<td>Warm Restart Ready</td>
<td>Whether the initial full checkpoint has finished</td>
<td>Yes or No</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Whether the running configuration on the backup unit includes all changes made on the management unit.</td>
<td>Current or Stale</td>
<td></td>
</tr>
</tbody>
</table>
Example
The `show nsf` command is used to display which unit is the management unit and which is the backup unit.

```
console#show nsf

Administrative Status.......................... Enable
Operational Status.............................. Enable
Last Startup Reason............................ Warm Auto-Restart
Time Since Last Restart......................... 0 days 16 hrs 52 mins 55 secs
Restart In Progress............................ No
Warm Restart Ready............................. Yes

Copy of Running Configuration to Backup Unit:
  Status...................................... Stale
  Time Since Last Copy........................ 0 days 4 hrs 53 mins 22 secs
  Time Until Next Copy......................... 28 seconds

<table>
<thead>
<tr>
<th>Unit</th>
<th>NSF Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**show power-usage-history**

Use the `show power-usage-history` command to display the history of unit power consumption for the unit specified in the command and total stack power consumption. Historical samples are not saved across switch reboots/reloads.
Syntax

show power-usage-history <unit-id>

- unit-id—Stack unit for which to display the power history. Range 1-12.

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

Power draw is measured at the power supplies. Power draw is not measured at the interfaces.

This command is not available on the Dell EMC Networking N1100-ON Series switches.

Example

console#show power-usage-history 1

Sampling Interval (sec)........................ 30
Total No. of Samples to Keep................... 168
Current Power Consumption (Watts)............. 56.2

<table>
<thead>
<tr>
<th>Sample No.</th>
<th>Time Since The Sample Was Recorded</th>
<th>Power Consumption On This Unit (Watts)</th>
<th>Power Consumption Per Stack (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>00:00:00:13</td>
<td>56.2</td>
<td>56.2</td>
</tr>
<tr>
<td>2</td>
<td>00:00:00:43</td>
<td>56.2</td>
<td>56.2</td>
</tr>
<tr>
<td>1</td>
<td>00:00:01:12</td>
<td>54.3</td>
<td>54.3</td>
</tr>
</tbody>
</table>

show process app-list

Use the show process app-list command to display the system applications.
**Syntax**

show process app-list

**Default Configuration**

This command does not have a default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Application ID assigned by the Process Manager.</td>
</tr>
<tr>
<td>Name</td>
<td>Application Name</td>
</tr>
<tr>
<td>PID</td>
<td>Application Linux Process ID.</td>
</tr>
<tr>
<td>Admin-Status</td>
<td>Flag indicating if the application is administratively enabled.</td>
</tr>
<tr>
<td>Auto-Restart</td>
<td>Flag indicating if the Process Manager should automatically restart the application if the application fails.</td>
</tr>
<tr>
<td>Running-Status</td>
<td>Flag indicating if the application is running.</td>
</tr>
</tbody>
</table>

**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console#show process app-list

ID  Name       PID  Admin  Auto  Running
    switchdrvr 280  Enabled  Enabled  Running
```
show process app-resource-list

This command lists the configured and in-use resources for each application known to the Process Manager.

Syntax
show process app-resource-list

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
The following fields are displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Application ID assigned by the Process Manager.</td>
</tr>
<tr>
<td>Name</td>
<td>Application Name</td>
</tr>
<tr>
<td>PID</td>
<td>Application Linux Process ID.</td>
</tr>
<tr>
<td>Memory-limit</td>
<td>Configured memory limit for the application, in Megabytes.</td>
</tr>
<tr>
<td>CPU Share</td>
<td>Configured CPU share in terms of percentage</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Current memory usage by this application, in Megabytes</td>
</tr>
<tr>
<td>Max Memory Usage</td>
<td>Maximum memory usage by this application, in Megabytes.</td>
</tr>
</tbody>
</table>
Command History

Introduced in version 6.2.0.1 firmware.

Example

console#show process app-resource-list

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>PID</th>
<th>Limit</th>
<th>Share</th>
<th>Usage</th>
<th>Max Mem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switchdrvr</td>
<td>280</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>256MB</td>
<td>280MB</td>
</tr>
<tr>
<td>2</td>
<td>syncdb-test</td>
<td>0</td>
<td>10MB</td>
<td>20%</td>
<td>0MB</td>
<td>0MB</td>
</tr>
</tbody>
</table>

show process cpu

Use the `show process cpu` command to check the CPU utilization for each process currently running on the switch.

Syntax

show process cpu

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

No specific guidelines.

Example

console#show process cpu

Memory Utilization Report

<table>
<thead>
<tr>
<th>status</th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>free</td>
<td>64022608</td>
</tr>
<tr>
<td>alloc</td>
<td>151568112</td>
</tr>
</tbody>
</table>
CPU Utilization:

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>5 Sec</th>
<th>1 Min</th>
<th>5 Min</th>
</tr>
</thead>
<tbody>
<tr>
<td>328bb20</td>
<td>tTffsPTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.02%</td>
</tr>
<tr>
<td>3291820</td>
<td>tNetTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>3295410</td>
<td>tXbdService</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.03%</td>
</tr>
<tr>
<td>347dcd0</td>
<td>ipnetd</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>348a440</td>
<td>osapiTimer</td>
<td>1.20%</td>
<td>1.43%</td>
<td>1.21%</td>
</tr>
<tr>
<td>350ee70</td>
<td>bcmL2X.0</td>
<td>0.40%</td>
<td>0.30%</td>
<td>0.12%</td>
</tr>
<tr>
<td>359d2e0</td>
<td>bcmCNTR.0</td>
<td>0.80%</td>
<td>0.42%</td>
<td>0.50%</td>
</tr>
<tr>
<td>3b5b750</td>
<td>bcmRX</td>
<td>0.00%</td>
<td>0.13%</td>
<td>0.12%</td>
</tr>
<tr>
<td>3d3f6d0</td>
<td>MAC Send Task</td>
<td>0.00%</td>
<td>0.07%</td>
<td>0.10%</td>
</tr>
<tr>
<td>3d48bd0</td>
<td>MAC Age Task</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.03%</td>
</tr>
<tr>
<td>40fdbf0</td>
<td>bcmLINK.0</td>
<td>0.00%</td>
<td>0.14%</td>
<td>0.46%</td>
</tr>
<tr>
<td>4884e70</td>
<td>tL7Timer0</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.02%</td>
</tr>
<tr>
<td>48a1250</td>
<td>osapiMonTask</td>
<td>0.00%</td>
<td>0.32%</td>
<td>0.17%</td>
</tr>
<tr>
<td>4969790</td>
<td>BootP</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>4d71610</td>
<td>dtlTask</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.05%</td>
</tr>
<tr>
<td>4ed00e0</td>
<td>hapiRxTask</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.03%</td>
</tr>
<tr>
<td>562e810</td>
<td>DHCP snoop</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.06%</td>
</tr>
<tr>
<td>58e9bc0</td>
<td>Dynamic ARP Inspection</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.03%</td>
</tr>
<tr>
<td>62038a0</td>
<td>dot1s_timer_task</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.03%</td>
</tr>
<tr>
<td>687f360</td>
<td>dot1xTimerTask</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.07%</td>
</tr>
<tr>
<td>6e23370</td>
<td>radius_task</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>6e2c870</td>
<td>radius_rx_task</td>
<td>0.00%</td>
<td>0.06</td>
<td>0.03%</td>
</tr>
<tr>
<td>7bc9030</td>
<td>spmTask</td>
<td>0.00%</td>
<td>0.09%</td>
<td>0.01%</td>
</tr>
<tr>
<td>7c58730</td>
<td>ipMapForwardingTask</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.03%</td>
</tr>
<tr>
<td>7f66e0</td>
<td>tRtrDiscProcessingTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>b1516d0</td>
<td>dnsRxTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
<tr>
<td>b194d60</td>
<td>tCptvPrtl</td>
<td>0.00%</td>
<td>0.06%</td>
<td>0.03%</td>
</tr>
<tr>
<td>b585770</td>
<td>isdpTask</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.02%</td>
</tr>
<tr>
<td>bda6210</td>
<td>RMONTask</td>
<td>0.00%</td>
<td>0.11%</td>
<td>0.11%</td>
</tr>
<tr>
<td>bdb24b0</td>
<td>boxs Req</td>
<td>0.00%</td>
<td>0.13%</td>
<td>0.10%</td>
</tr>
<tr>
<td>c2d6db0</td>
<td>sshd</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.01%</td>
</tr>
</tbody>
</table>

Total CPU Utilization 2.40% 3.62% 3.45%

**show process proc-list**

This command lists the configured and in-use resources for each application known to the Process Manager.
**Syntax**

show process proc-list

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The following fields are displayed.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Application Linux Process ID</td>
</tr>
<tr>
<td>Process-Name</td>
<td>Linux process name</td>
</tr>
<tr>
<td>Application ID-VRID-Name</td>
<td>Name of the application that started the process and the application ID assigned by the Process Manager. The VRID is the virtual router with which this application is associated. The VRID is 0 for processes associated with the default router and on platforms which do not support the virtual routing feature.</td>
</tr>
<tr>
<td>Child</td>
<td>Flag indicating if this process is started directly by the Process Manager or if it is a child process started by the application process.</td>
</tr>
<tr>
<td>VM Size</td>
<td>Virtual Memory consumed by this process in Kilobytes</td>
</tr>
<tr>
<td>VM Peak</td>
<td>Maximum Virtual Memory consumed by this process in Kilobytes</td>
</tr>
<tr>
<td>FD Count</td>
<td>Number of file descriptors open in this process.</td>
</tr>
</tbody>
</table>
**Command History**

Introduced in version 6.2.0.1 firmware.

**Example**

```
console##show process proc-list
```

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>ID-VRID-Name</th>
<th>Child</th>
<th>VM Size (KB)</th>
<th>VM Peak (KB)</th>
<th>FD Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>280</td>
<td>switchdrvr</td>
<td>1-0-switchdrvr</td>
<td>No</td>
<td>220992</td>
<td>230724</td>
<td>36</td>
</tr>
<tr>
<td>281</td>
<td>syncdb</td>
<td>2-0-syncdb</td>
<td>No</td>
<td>2656</td>
<td>2656</td>
<td>8</td>
</tr>
<tr>
<td>281</td>
<td>proctest</td>
<td>3-55-proctest</td>
<td>No</td>
<td>2656</td>
<td>2656</td>
<td>8</td>
</tr>
</tbody>
</table>

**show router-capability**

Use this command to display the router capabilities of the loaded firmware image.

**Syntax**

```
show router-capability
```

**Command Mode**

Privileged Exec mode, Global Configuration mode and all sub-modes.

**User Guidelines**

The capabilities in the switch firmware are determined during the build process.

**Command History**

Introduced in version 6.3.0.1 firmware. Updated in version 6.5 firmware.

**Examples**

This example displays the capabilities of an N3000v6.5.x.x firmware build.

```
console# show router-capability
This firmware supports a stack of up to twelve switches. MVRP/MMRP capabilities and up to 4093 VLANs may be configured.
```
This example displays the capabilities of an N3000BGPv6.3.x.x firmware mixed stacking build.

console#show router-capability
This firmware supports a stack of up to eight switches. MVRP/MMRP capabilities are not available.

**show sessions**

Use the `show sessions` command to display a list of the open sessions from remote hosts.

**Syntax**

`show sessions`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays a list of open sessions from remote hosts.

```
console#show sessions
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User Name</th>
<th>Connection from</th>
<th>Idle Time</th>
<th>Session Time</th>
<th>Session Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>EIA-232</td>
<td></td>
<td>00:00:00</td>
<td>00:01:03</td>
<td>Serial</td>
</tr>
<tr>
<td>1</td>
<td>admin</td>
<td>10.130.128.17</td>
<td>00:00:05</td>
<td>00:00:10</td>
<td>Telnet</td>
</tr>
<tr>
<td>11</td>
<td>admin</td>
<td>10.27.192.56</td>
<td>00:00:27</td>
<td>00:00:28</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.
show slot

Use the show slot command to display information about all the slots in the system or detailed information for a specific slot.

Syntax

show slot [slot/port]

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

Switch slots are populated with cards (see the show supported cardtype command below). However, not all slots are available to be externally populated. Slots which may be populated in the field are marked as pluggable. Every switch has a least one slot, which is populated with the base switching card. Systems with an external CPU will show an additional slot which is populated with the external CPU. Both of these slots are marked as non-pluggable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>The session identifier. Use with the disconnect command.</td>
</tr>
<tr>
<td>User Name</td>
<td>The login ID associated with the session.</td>
</tr>
<tr>
<td>Connection from</td>
<td>The origin of the connection.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>The elapsed time since session activity was last detected.</td>
</tr>
<tr>
<td>Session Time</td>
<td>The elapsed time since the session was connected.</td>
</tr>
<tr>
<td>Session Type</td>
<td>The type of connection (Serial, Telnet, SSH, HTTP, HTTPS).</td>
</tr>
</tbody>
</table>
The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>The slot identifier in a slot/port format.</td>
</tr>
<tr>
<td>Slot Status</td>
<td>The slot is empty, full, or has encountered an error.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The slot administrative mode is enabled or disabled.</td>
</tr>
<tr>
<td>Power State</td>
<td>The slot power mode is enabled or disabled.</td>
</tr>
<tr>
<td>Configured Card Model Identifier</td>
<td>The model identifier of the card preconfigured in the slot. Model identifier is a 32-character field used to identify a card.</td>
</tr>
<tr>
<td>Pluggable</td>
<td>Cards are pluggable or non-pluggable in the slot.</td>
</tr>
</tbody>
</table>

If you supply a value for slot/port, the following additional information appears as shown in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inserted Card Model Identifier</td>
<td>The model identifier of the card inserted in the slot. Model identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.</td>
</tr>
<tr>
<td>Inserted Card Description</td>
<td>The card description. This field is displayed only if the slot is full.</td>
</tr>
<tr>
<td>Configured Card Description</td>
<td>The description of the card preconfigured in the slot.</td>
</tr>
</tbody>
</table>

**Example**

```
console>show slot
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Status</th>
<th>State</th>
<th>Power</th>
<th>State</th>
<th>Configured Card Model ID</th>
<th>Pluggable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Command History
Description updated in the 6.4 release.

show supported cardtype

Use the show supported cardtype command to display information about all card types supported in the system.

Syntax
show supported cardtype [cardindex]

- cardindex — Displays the index into the database of the supported card types. This index is used when preconfiguring a slot.

Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
If a card index is entered, then the command displays information about specific card types supported in the system. Card index values are specific to each family of products. Use the generic form (without specifying an index) to display all the card types for a product family.

The CID information is used when preconfiguring cards using the slot command.

The following table explains the output parameters.
If you supply a value for cardindex, the following additional information appears as shown in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Index (CID)</td>
<td>The index into the database of the supported card types. This index is used when preconfiguring a slot.</td>
</tr>
<tr>
<td>Card Model Identifier</td>
<td>The model identifier for the supported card type.</td>
</tr>
</tbody>
</table>

If you supply a value for cardindex, the following additional information appears as shown in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Type</td>
<td>The 32-bit numeric card type for the supported card.</td>
</tr>
<tr>
<td>Model Identifier</td>
<td>The model identifier for the supported card type.</td>
</tr>
<tr>
<td>Card Description</td>
<td>The description for the supported card type.</td>
</tr>
</tbody>
</table>

**Example**

This example shows the supported card types for the Dell EMC Networking N4000 switch.

```
console>show supported cardtype

CID    Card Model ID
---    ----------------------------------------
1      XLP308 Base CPU Card
2      Dell Networking N4032
3      Dell Networking N4032F
4      Dell Networking N4064
5      Dell Networking N4064F
6      Dell QSFP Card
7      Dell SFP+ Card
8      Dell 10GBase-T Card
```

**Command History**

Description updated in the 6.4 release.
show supported switchtype

Use the show supported switchtype command to display information about all supported switch types.

Syntax

show supported switchtype [switchindex]

- switchindex — Specifies the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. (Range: 0–65535)

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

The switch SID is used when preconfiguring switches in a stack using the member command in config-stack mode.

The following table describes the fields in the first example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Index (SID)</td>
<td>This field displays the index into the database of supported switch types.</td>
</tr>
<tr>
<td></td>
<td>This index is used when preconfiguring a member to be added to the stack.</td>
</tr>
<tr>
<td>Model Identifier</td>
<td>This field displays the model identifier for the supported switch type.</td>
</tr>
<tr>
<td>Management Preference</td>
<td>This field indicates the management preference value of the switch type.</td>
</tr>
<tr>
<td>Code Version</td>
<td>This field displays the code load target identifier of the switch type.</td>
</tr>
</tbody>
</table>
The following table describes the fields in the second example.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Type</td>
<td>This field displays the 32-bit numeric switch type for the supported switch.</td>
</tr>
<tr>
<td>Model Identifier</td>
<td>This field displays the model identifier for the supported switch type.</td>
</tr>
<tr>
<td>Switch Description</td>
<td>This field displays the description for the supported switch type.</td>
</tr>
</tbody>
</table>

**Example**

The following example displays the information for supported switch types.

```bash
console# show supported switchtype
SID       Switch Model ID
---          -------------
 1   N4032
 2   N4032F
 3   N4064
 4   N4064F
```

The following example displays the format of the `show supported switchtype` command.

```bash
console# show supported switchtype 1

Switch Type....................... 0xd8420001
Model Identifier.................. N4032
Switch Description.............. Dell Networking N4032

Supported Cards:
  Slot......................... 0
  Card Index (CID)............. 1
  Model Identifier............. Dell Networking N4032

  Slot......................... 1
  Card Index (CID)............. 5
  Model Identifier............. Dell QSFP Card

  Slot......................... 1
  Card Index (CID)............. 6
  Model Identifier............. Dell SFP+ Card

  Slot......................... 1
```
show switch

Use the show switch command to display information about units in the stack.

Syntax

show switch [stack–member–number | stack–ports[counters | diag | stack-path {from-unit | all} to-unit] | stack–standby]

- stack–member–number—The stack member number.
- stack–ports—Display summary stack-port information for all interfaces.
- counters—Display summary data counter information for all interfaces.
- diag—Display front panel stacking diagnostics for each port.
- stack-path—Display the active path from one stacking unit to another.
- From-unit—The unit from which the packets originate.
- all—Displays all unit paths.
- To-unit—The unit to which the packets are sent.
- stack–standby—Display the configured or automatically selected standby unit number.

Default Configuration

This command has no default configuration.

Command Mode

User Exec, Privileged Exec, Global Configuration mode and all Configuration submodes

User Guidelines

The show switch command shows the configuration and status of the stacking units, including the active and standby stack management units, the pre-configured model identifier, the plugged in model identifier, the switch
status and the current code version. Both the pre-configured switch types (as set by the `member` command in stack mode) and the currently connected switch types, if any, are shown.

The `show switch stack-member-number` command also shows details of the switch configuration including the SFS last attempt status for the specified unit. If there is a stack firmware synchronization (SFS) operation in progress, the switch status will show as **Updating Code**.

The `show switch` command may show an SDM Mismatch value in the Switch Status field. This value indicates that the unit joined the stack, but is running a different SDM template than the management unit. This status should be temporary; the stack unit should automatically reload using the template running on the stack manager.

Use the `show supported switchtype` command to display switch SIDs.

Use the `show switch stack-ports` command to display details regarding stacking links.

Use the `show slot` command to display details regarding slot configuration.

Use the `show sdm prefer` command to display the SDM template configuration.

The `show switch stack-ports stack-path` command is useful in tracking the path a packet may take when traversing stacking links. The command shows active paths only, not those that may be taken after a stack failover or stack reconvergence.

The following table describes the fields in the switch stack status example.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>This field displays the unit identifier assigned to the switch.</td>
</tr>
<tr>
<td>Management Status</td>
<td>This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.</td>
</tr>
<tr>
<td>Switch Type</td>
<td>This field displays the 32-bit numeric switch type.</td>
</tr>
<tr>
<td>Preconfigured Model Identifier</td>
<td>This field displays the model identifier for this switch. Model Identifier is a 32-character field assigned by Dell to identify the switch.</td>
</tr>
</tbody>
</table>
The additional fields in the all units example are as follows:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugged-in Model Identifier</td>
<td>This field displays the model identifier for this switch. Model Identifier is a 32-character field assigned by Dell to identify the switch. If no physical unit is present for the unit number, this field is empty.</td>
</tr>
<tr>
<td>Switch Status</td>
<td>This field displays the switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, SDM Mismatch Not Present, Updating Code, or STM Mismatch</td>
</tr>
<tr>
<td>Switch Description</td>
<td>This field displays the switch description.</td>
</tr>
<tr>
<td>Detected Code Version</td>
<td>This field displays the version of code running on this switch. If the switch is not present and the data is from preconfiguration, the code version is “None.”</td>
</tr>
<tr>
<td>Detected Code in Flash</td>
<td>This field displays the version of code that is currently stored in FLASH memory on the switch. This code will execute after the switch is reset. If the switch is not present and the data is from preconfiguration, then the code version is “None.”</td>
</tr>
<tr>
<td>SFS Last Attempt Status</td>
<td>This field displays the Stack Firmware Synchronization status. The possible values are: Success, Failure, Min bootcode version not present, None.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>This field displays the Switch serial number.</td>
</tr>
<tr>
<td>Up Time</td>
<td>This field displays the system up time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>This field displays the unit identifier assigned to the switch.</td>
</tr>
<tr>
<td>Management Status</td>
<td>This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.</td>
</tr>
</tbody>
</table>
Per Unit Status Parameters are explained as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF Support</td>
<td>Whether a unit supports NSF</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Examples**

**Example – Stack Status for the Switch**

```
cache#show switch 1
Switch............................ 1
Management Status............... Management Switch
Switch Type....................... 0xd8460001
Preconfigured Model Identifier.. N4064
Plugged-in Model Identifier..... N4064
Switch Status................... OK
Switch Description............... Dell Networking N4064
Detected Code Version............ 6.0.0.0
Detected Code in Flash........... 6.0.0.0
SFS Last Attempt Status......... None
```
Example-Stack Ports

This example displays information about the stack ports.

```
console#show switch stack-ports
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Stack Mode</th>
<th>Stack Mode</th>
<th>Link Status</th>
<th>Link Speed (Gb/s)</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tw1/0/1</td>
<td>Stack</td>
<td>Stack</td>
<td>Link Down</td>
<td>21</td>
<td>Enabled</td>
</tr>
<tr>
<td>Tw1/0/2</td>
<td>Stack</td>
<td>Stack</td>
<td>Link Up</td>
<td>21</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tw2/0/1</td>
<td>Stack</td>
<td>Stack</td>
<td>Link Down</td>
<td>21</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tw2/0/2</td>
<td>Stack</td>
<td>Stack</td>
<td>Link Up</td>
<td>21</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Example – All Units in the Stack

This example displays information about all units in the stack.

```
console>show switch
```

<table>
<thead>
<tr>
<th>SW</th>
<th>Status</th>
<th>Management Status</th>
<th>Preconfig Model ID</th>
<th>Plugged-in Model ID</th>
<th>Switch Status</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mgmt Sw</td>
<td>OK</td>
<td>N3048</td>
<td>N3048</td>
<td>OK</td>
<td>6.0.0.0</td>
</tr>
</tbody>
</table>

Example-Stacking Links Path

This command tracks the path a packet may take when traversing stacking links. The command shows active paths only, not those that may be taken after a stack failover or stack reconvergence.

```
console#show switch stack-ports stack-path 3 1
```

Packet-path from unit 3 to unit 1:

1. unit-3 port gi3/0/49 to unit-2
2. unit-2 port gi2/0/49 to unit-1

Example – Switch Firmware Stack Status

The following example displays the Switch Firmware stack status information for the switch.

```
console#show switch
```

<table>
<thead>
<tr>
<th>SW Switch Status</th>
<th>Preconfig Model ID</th>
<th>Plugged-in Model ID</th>
<th>Switch Status</th>
<th>Code Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
console#show switch 1

Switch............................ 1
Management Status................ Management Switch
Switch Type....................... 0x63400004
Preconfigured Model Identifier... N3048P
Plugged-in Model Identifier..... N3048P
Switch Status..................... OK
Switch Description................. Dell Networking N3048P
Detected Code Version............. 6.0.0.0
Detected Code in Flash............ 6.0.0.0
SFS Last Attempt Status......... None
Serial Number..................... 13820M0230LF
Up Time........................... 0 days 3 hrs 1 mins 13 secs

Example – SDM Templates
This example shows the SDM Mismatch value in the Switch Status field.

console(config)#show switch

show system
Use the show system command to display system information.

Syntax
show system [unit]
  •  unit — The unit number.

Default Configuration
This command has no default configuration.
**Command Mode**
User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The temperature and power sections are only displayed for switches that have temperature or power monitoring capability.

**Example**

```
console#show system

System Description: Dell Networking Switch
System Up Time: 0 days, 03h:02m:30s
System Contact:
System Name:
System Location:
Burned In MAC Address: 001E.C9DE.B41B
System Object ID: 1.3.6.1.4.1.674.10895.3060
System Model ID: N3048P
Machine Type: Dell Networking N3048P

System Thermal Conditions:

Unit Temperature State
(Celsius)
----- --------------
1 34 Good

Temperature Sensors:

Unit Description Temperature
Description (Celsius)
----- ---------------
1 MAC 33
1 PHY 34

Fans:

Unit Description Status
----- --------------
1 Fan-1 Failure
1 Fan-2 Failure

Power Supplies:
```
### Unit Description Commands

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
<th>Status</th>
<th>Average Power (Watts)</th>
<th>Current Power (Watts)</th>
<th>Since Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System</td>
<td>Non-critical</td>
<td>39.8</td>
<td>39.8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>PS-1</td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>PS-2</td>
<td>No Power</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/1970 00:00:00</td>
</tr>
</tbody>
</table>

**USB Port Power Status:**
Device Not Present

### show system fan

Use the `show system fan` command to explicitly display the fan status.

**Syntax**

```
show system fan
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

```
console>show system fan
Fans:
Unit Description Status
---- ----------- ------
1  Fan 1       OK
1  Fan 2       OK
1  Fan 3       OK
```
**show system id**

Use the `show system id` command to display the system identity information.

**Syntax**

```
show system id [unit]
```

- **unit** — The unit number.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The tag information is on a switch by switch basis.

**Example**

The following example displays the system service tag information.

```
console#show system id

Service Tag: at-N3024-X00-0010
Serial Number: sn-a128
Asset Tag:

Unit Service tag       Serial number           Asset tag
---- ------------      --------------          ------------
1   at-N3024-X00-0010 sn-a128
```

**show system power**

Use the `show system power` command to display information about the system level power consumption.

**Syntax**

```
show system power
```
Default Configuration
This command has no default configuration.

Command Mode
User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines
This command is only available on switches with a power monitoring circuit. It is not available on the Dell EMC Networking N1100-ON Series switches.

Examples
console#show system power

Power Supplies:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
<th>Status</th>
<th>Average Power (Watts)</th>
<th>Current Power (Watts)</th>
<th>Since Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System</td>
<td>Non-critical</td>
<td>39.8</td>
<td>39.8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>PS-1</td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>PS-2</td>
<td>No Power</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/1970 00:00:00</td>
</tr>
</tbody>
</table>

show system temperature

Use the show system temperature command to display information about the system temperature and fan status.

Syntax
show system temperature

Default Configuration
This command has no default configuration.
**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes.

**User Guidelines**

The system temperature is read from one or more sensors placed at critical locations on the PCB. Status ranges are subdivided into Ok (Cool), Non-critical (Warm), and Critical (Hot). Each status range has a lower, mid-range, and upper limit with the upper limit of the lower temperature status being the same as the lower limit of the adjacent higher temperature status. Within a range, the fans run at a reduced speed for the lower temperature part of the range and an increased speed for the higher temperature part of the range. Each range runs the fans at increasingly higher speeds for increasingly higher temperatures. Above the Critical status upper limit, the system is shut down. Typically, the shutoff temperature for the switch is 90-105°C.

To avoid fan speed oscillation around a temperature limit, a small hysteresis is added to the limit such that the temperature for increasing the fan speed is higher than the temperature for lowering the fan speed. This implies that the higher fan speed (and status) is maintained until the switch is cooled 3-5 degrees below the threshold for increasing the fan speed (and possibly changing the status). The exact thresholds for increasing or lowering the fan speed are determined during thermal analysis and are different for each switch family.

**Examples**

```
console#show system temperature

System Thermal Conditions:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Temperature</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Celsius)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>34</td>
<td>OK</td>
</tr>
</tbody>
</table>

Temperature Sensors:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(Celsius)</td>
</tr>
<tr>
<td>1</td>
<td>MAC</td>
<td>33</td>
</tr>
</tbody>
</table>
```
**show tech-support**

Use the `show tech-support` command to display system and configuration information for use in debugging or contacting technical support. The output of the `show tech-support` command combines the output of the following commands:

- show interfaces transceiver
- show power inline
- show switch stack-port counters
- show nsf
- show slot
- show interfaces advertise
- show interfaces advanced firmware
- show lldp remote-device all
- show interfaces counters errors
- show fiber-ports optical-transceiver
- show process cpu
- show ethernet cfm errors (N4000 series only)
- show power inline firmware-version
- show version
- show interfaces transceiver properties

**Syntax**

```
show tech-support [ bgp | bgp-ipv6 | ospf | ospfv3 | bfd ] [file | usb]
```

- **bgp** — Show detailed information specific to BGP.
- **bgp-ipv6** — Show detailed information specific to BGP IPv6.
- **ospf** — Show detailed information specific to OSPF.
- **ospfv3** — Show detailed information specific to OSPFv3.
- **bfd** — Show detailed information specific to BFD.
- **file** — Write the output to a file in the local flash instead of the console.
• **usb** — Write the output to a file on the USB drive instead of the console. A USB storage device must be inserted into the front panel USB port.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

The output of the show tech-support command combines the output of the following commands at a minimum:

- show interfaces transceiver
- show power inline
- show switch stack-port counters
- show nsf
- show slot
- show interfaces advertise
- show interfaces advanced firmware
- show lldp remote-device all
- show interfaces counters errors
- show fiber-ports optical-transceiver
- show process epu
- show ethernet cfm errors (N4000 series only)
- show power inline firmware-version
- show version
- show interfaces transceiver properties

Tech support files are named tech-supportXXX.txt, where XXX is the date and time stamp of the form YYMMDHHMSS. YY is the last two digits of the year, MM is the month, DD is the day of the month, HH is the hour in 24-hour format, MM is the minute, and SS is the second.

Use the copy flash:///techsupportXXX.txt <destination> form of the copy command to copy the tech-support file from the switch.
A USB device must be plugged in to the USB port, and cleanly mounted, if the `usb` parameter is given.

**Default Value**

This command has no defaults.

**Example**

```
console#show tech-support

***************** Show Version ******************
Switch: 1

System Description.............. Dell Networking N4032, 6.0.0.0, Linux 2.6.32.9

Machine Description............. Dell Networking Switch
System Model ID................... N4032
Machine Type..................... Dell Networking N4032
Serial Number................... 0000
Manufacturer.................... 0xbc00
Operating System............... Linux 2.6.32.9
Burned In MAC Address.......... 0011.2233.4455
System Object ID................ 1.3.6.1.4.1.674.10895.3042
CPU Version...................... XLP308H-B2
SOC Version..................... BCM56842_A1
HW Version...................... 3
CPLD Version.................... 17

unit active backup current-active next-active
---- ----------- ----------- -------------- --------------
1 6.0.0.0 <none> 6.0.0.0 6.0.0.0

Operating System................ Linux 2.6.32
Additional Packages............... FTOS QoS
                                  FTOS Multicast
                                  FTOS Stacking
                                  FTOS Routing
                                  FTOS Data Center

***************** Show SysInfo ******************
System Location............................
System Contact..............................
System Object ID.......................... 1.3.6.1.4.1.674.10895.3042
System Up Time............................. 0 days 0 hrs 14 mins 53 secs
10/100 Ethernet/802.3 interface(s)........ 1
Gig Ethernet/802.3 interface(s)............ 0
10Gig Ethernet/802.3 interface(s)......... 0
40Gig Ethernet/802.3 interface(s)......... 0
Virtual Ethernet/802.3 interface(s)....... 1

System Thermal Conditions:
The following example writes the tech-support output to a file on a USB stick.

console#show tech-support usb

**Command History**
Description updated in the 6.4 release.

**show users**
Use the **show users** command to display information about the active users.

**Syntax**

```
show users [long]
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**
The command also shows which administrative profiles have been assigned to local user accounts and to show which profiles are active for logged-in users.

**Example**
The following example displays a list of active users and the information about them.
show version

Use the show version command in User Exec mode to displays the system version information.

Syntax

show version [unit ]

- unit — The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

User Guidelines

This command shows the version information for the stack master if no arguments are given.

Example

```
console#show version

Machine Description............... Dell Networking Switch
System Model ID................... N4064
Machine Type...................... Dell Networking N4064
```
Serial Number..................... X01-64C-55
Manufacturer...................... 0xbc00
Burned In MAC Address............. D067.E5C0.D19B
System Object ID.................. 1.3.6.1.4.1.674.10895.3045
CPU Version....................... XLP308H-A1
SOC Version....................... BCM56846_A1
HW Version......................... 3
CPLD Version....................... 14
Boot Version....................... v1.0.21
Image File......................... N4000v6.0.0.1
Software Capability............... Stack Limit = 12, VLAN Limit = 4093

<table>
<thead>
<tr>
<th>unit</th>
<th>active</th>
<th>backup</th>
<th>current-active</th>
<th>next-active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.0.0.1</td>
<td>5.1.0.1</td>
<td>6.0.0.1</td>
<td>5.1.0.1</td>
</tr>
</tbody>
</table>

console#show version 2

SOC Version....................... BCM56842_B1
HW Version......................... 1
CPLD Version....................... 14
Boot Version....................... v1.0.21

<table>
<thead>
<tr>
<th>Unit</th>
<th>Image 1</th>
<th>Image 2</th>
<th>Current Active</th>
<th>Next Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6.0.0.1</td>
<td>5.1.0.1</td>
<td>6.0.0.1</td>
<td>6.0.0.1</td>
</tr>
</tbody>
</table>

stack

Use the stack command in Global Configuration mode to enter Stack Configuration mode.

Syntax

stack

Default Configuration

This command has no default mode.

Command Mode

Global Configuration mode
User Guidelines

If no stack configuration appears in the saved config, it is built at runtime and appears in the running config. The operator can save the stack configuration. Switches that do not match the saved config (are of a different type than as configured) after a reboot will show a config mismatch and do not join the stack. Units that do not join the stack will show their interfaces as detached.

Example

The following example sets the console command mode to Stack Config.

```
console(config)#stack
console(config-stack)#
```

stack-port

Use the `stack-port` command in Stack Configuration mode to configure ports as either Stacking ports or as Ethernet ports.

⚠️ **NOTE:** This command is only valid on the N1100-ON, N1500 and N4000 switches. It issues an error response if used on the N2000, N2100-ON, N3000-ON, or N3100 switches.

Syntax

```
stack-port {fortygigabitethernet|twentygigabitethernet|tengigabitethernet} unit/slot/port {ethernet|stack [speed {40g|21g}]}
```

- `speed {40g|21g}`—Set the stack port speed. The speed parameter is only available on the Dell EMC Networking N2100/N3100 Series switches.

Default Configuration

By default, Ethernet ports are configured to operate in Ethernet mode. The default stack port speed on the Dell EMC Networking N2100/N3100 Series switches is 21 Gigabit.

Command Mode

Stack Configuration mode
**User Guidelines**

This command is used to configure Ethernet ports to operate as either stacking or Ethernet ports, or to configure stacking modules to operate as Ethernet ports.

Once this command has been issued, the switch must be rebooted in order for the command to take effect. Issuing multiple stack-port commands for a single interface without intervening reboots results in undefined behavior and is not supported. Reboot the switch and examine the output of the `show switch stack-ports` command to determine the active configuration. The `clear config` command does not change the stacking port mode. Only the `stack-port` command can change the operating mode of the stacking port and it only takes effect after a reboot.

The stack-port configuration mode does not appear in the running config. Use the `show switch stack-port` command to display configuration and status of stacking ports. Ports that are configured to operate as stacking ports will show as detached in the `show interfaces status` command output.

Use the `show switch` command to display information regarding the switches in a stack. Fortygigabitethernet ports are only supported on the N4000 series switches. Redundant stacking links between any two units must operate at the same speed. A 40G port configured in 4x10G mode is considered to be operating at 10G speed.

Up to eight stack ports can be configured per stacking unit (four in each direction).

The N4000 Series switches support up to twelve units configured in a stack and can utilize 10GBaseT, SFP+ or QSFP connections for stacking. The N2000/N2100-ON/N3000/N3100-ON Series switches support up to twelve units configured in a stack and can only utilize the rear panel mini-SAS ports for stacking. The N1100-ON and N1500 Series switches support stacking up to four units in a stack and can utilize pairs of SFP+ ports for stacking.

On the N1100-ON/N1500 Series switch, configuring an SFP+ port as stacking will always configure the adjacent port on the unit being configured in stacking mode as well (i.e., configuring Te1/0/1 as stacking configures Te1/0/2 as stacking and configuring Te1/0/3 as stacking configures Te1/0/4 as stacking).
Changing the stacking link speed requires a reboot of the affected switch. 21G stacking is not compatible with 40G stacking. All stacking links in a stack must be configured to use the same speed.

Changing the speed of one stacking link changes the speed on the adjacent stack port on the switch being configured as well. The connected switch stack port(s) must be similarly configured. It is not possible to operate the stacking links on a switch at different speeds. Clearing the configuration does not affect the stack port speed settings.

**Command History**

Added the speed parameter in version 6.5.

**Example**

core@switch#stack-port tengigabitethernet 1/0/3 stack

core@switch(config-stack)#stack-port shutdown

Use this command to enable or disable the stack port administratively. This command is usually used to diagnose the stack in case any one of the stack ports is exhibiting errors.

**Syntax**

```
stack-port interface-id shutdown
no stack-port interface-id shutdown
```

- **interface-id**—The stacking interface identifier.

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Stack Configuration mode
**User Guidelines**

This command must be used with caution, as disabling a stack port causes the stack to attempt to reconverge. Ensure that the stack is in an active ring topology in order to avoid a stack split. Check the stack ports for errors and also verify that NSF is synced before shutting down any stacking links. Application messages will appear in the logs during stack convergence.

This command persists across reboots, therefore, administrators should use this command with caution during stack upgrade procedures.

**Example**

console(config-stack)#stack-port tengigabitethernet 1/2/1 shutdown

Disabling a stack port will cause the stack to attempt to re-converge. Application messages will appear in the logs during stack convergence.

Before shutting down a stack link, please ensure that your stack is in an active ring topology in order to avoid a stack split. Continue? (y/n)

console(config-stack)#no stack-port twentygigabitethernet 1/0/1 shutdown

**standby**

Use the **standby** command to configure the standby unit in the stack. This unit comes up as the master when the stack failover occurs. Use the **no** form of this command to reset to default, in which case, a standby is automatically selected from the existing stack units if there no preconfiguration.

**Syntax**

`standby unit`

`no standby`

- **unit** — Valid unit number in the stack. (Range: 1–12 maximum (less on stacks with a restricted stack size, for example, AdvLite). The range is limited to the number of units available on the stack.)

**Default Configuration**

The default configuration is to allow the software to automatically select a standby unit.
**Command Mode**
Stack Configuration mode

**User Guidelines**
This unit comes up as the master when the stack failover occurs. Use the no form of this command to reset to default, in which case, a standby is automatically selected from the existing stack units if there is no preconfiguration.

**Examples**
```
console(config)#stack
console(config-stack)#standby 2
```

**Command History**
User Guidelines updated in the 6.4 release.

**switch renumber**
Use the `switch renumber` command in Global Configuration mode to change the identifier for a switch in the stack.

**Syntax**
```
switch oldunit renumber newunit
```
- `oldunit` — The current switch identifier. (Range: Dependent on Series/Model)
- `newunit` — The updated value of the switch identifier. (Range: Dependent on Series/Model)

**Command Mode**
Global Configuration mode

**User Guidelines**
Upon execution, the switch is configured with the configuration information for the new switch if any is available. The old switch configuration information is retained; however, the original switch will be operationally
detached. This means the interfaces show as detached in show interfaces status output and no switch type will show for the Plugged-in Model Id in the output of the show switch command.

This command may be executed on the stack master or a standalone unit. This command reboots the renumbered switch. After renumbering a switch, it is important to let the master switch synchronize the NSF state before proceeding with additional stack management operations. Use the show nsf command to check the NSF state. If the switch shows Warm Restart Ready as Yes, then the master switch state is synchronized with the standby switch. Failure to observe this caution may result in the master unit spontaneously resetting due to configuration mismatch in order to re-elect a master unit. The range of switch numbers is 1 to maximum stack size. The maximum stack size varies, depending on the switch model. The switch renumber command prompt will display the valid range.

Example

The following example displays how to reconfigure switch number “1” to an identifier of “2.”

console(config)#switch 1 renumber 2

telnet

Use the telnet command to log into a host that supports Telnet.

Syntax

telnet {ip-address | hostname} [port] [keyword1......]

- ip-address—Valid IP address of the destination host.
- hostname—Hostname of the destination host. (Range: 1–158 characters).
- port—A decimal TCP port number.
- keyword—One or more keywords from the keywords table in the user guidelines (see Keywords Table below).

Keywords Table

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
Switch Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/debug</td>
<td>Enable telnet debugging mode.</td>
</tr>
<tr>
<td>/line</td>
<td>Enable telnet linemode.</td>
</tr>
<tr>
<td>/localecho</td>
<td>Enable telnet localecho.</td>
</tr>
<tr>
<td>&lt;cr&gt;</td>
<td>Press ENTER to execute the command.</td>
</tr>
<tr>
<td>port</td>
<td>Enter the TCP port number.</td>
</tr>
</tbody>
</table>

**Default Configuration**

port — Telnet TCP port (decimal 23) on the host.

**Command Mode**

User Exec, Privileged Exec mode

**User Guidelines**

This command has no user guidelines.

**Example**

Following is an example of using the `telnet` command to connect to 176.213.10.50.

```
console#telnet 176.213.10.50
Trying 176.213.10.50...
Connected to 176.213.10.50
Entering character mode...
Escape character is'^'^'.
```

**traceroute**

Use the `traceroute` command to discover the routers that packets traverse when traveling to their destination.

**Syntax**

```
traceroute [vrf vrf-name] [ip] ipaddress|hostname [init-ttl initTtl] [max-ttl maxTtl] [max-fail maxFail] [interval interval] [count count] [port port] [size size][source {src-ip-address|vlan vlan-id|loopback loopback-id}]
```
- **vrf-name**—The name of the VRF associated with the routing table context used by the command. If no vrf is specified, the global routing table context is used.
- **ipaddress**—Valid IP address of the destination host.
- **hostname**—Hostname of the destination host. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, `console (config) #snmp-server host "host name"
- **initTtl**—The initial time-to-live (TTL); the maximum number of router hops between the local and remote system (Range: 1–255).
- **maxTtl**—The largest TTL value that can be used (Range: 1–255).
- **maxFail**—Terminate the traceroute after failing to receive a response for this number of consecutive probes (Range: 1–255).
- **interval**—The timeout period. If a response is not received within this period of time, then traceroute considers that probe a failure (printing * ) and sends the next probe. If traceroute does receive a response to a probe, then it sends the next probe immediately. (Range: 1–60 seconds).
- **count**—The number of probes to be sent at each TTL level (Range: 1–10).
- **port**—The destination UDP port of the probe. This should be an unused port on the remote destination system (Range: 1–65535).
- **size**—The size, in bytes, of the payload of the Echo Requests sent (Range: 0–39936 bytes).
- **src-ip-address**—The IPv4 source address to use in the ICMP echo request packets.
- **vlan-id**—A valid VLAN interface.
- **loopback-id**—A configured loopback ID

**Default Configuration**

The default count is 3 probes.
The default interval is 3 seconds.
The default size is 0 data bytes.
The default port is 33434.
The default initTtl is 1 hop.
The default maxTtl is 30 hops.
The default maxFail is 5 probes.

**Command Mode**
User Exec mode and Privileged Exec mode

**User Guidelines**
Use of the optional VRF parameter executes the command within the context of the VRF-specific routing table.

Traceroute operates by sending a sequence of Internet Control Message Protocol (ICMP) echo request packets. The time-to-live (TTL) value, is used in determining the intermediate routers through which the packet flows toward the destination address. Routers decrement a packet’s TTL value and discard packets whose TTL equals 0. On discarding a packet, the router returns an ICMP time exceeded message to the source.

The VRF identified in the parameter must have been previously created or an error is returned.

Only IPv4 addresses are supported with the `vrf` parameter. The `vrf` parameter is only available on the N3000/N3100/N4000 switches.

Loopback interfaces are not supported on the N1100-ON Series switches.

**Examples**
The following example discovers the routes that packets will actually take when traveling to the destination specified in the command.

```bash
(console)# traceroute 10.240.10.115 init-ttl 1 max-ttl 4 max-fail 0 interval 1 count 3 port 33434 size 43
Traceroute to 10.240.10.115, 4 hops max, 43 byte packets:
1 10.240.4.1 708 msec 41 msec 11 msec
2 10.240.10.115 0 msec 0 msec 0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

**Command History**
Syntax updated in 6.4 release.
**traceroute ipv6**

Use the `traceroute` command to discover the routers that packets traverse when traveling to their destination.

**Syntax**

```
traceroute [ipv6] ipv6address|hostname [init-ttl initTtl] [max-ttl maxTtl] [max-fail maxFail] [interval interval] [count count] [port port] [size size] [source {src-ip-address|vlan vlan-id|loopback loopback-id}]
```

- `ipv6address`—Valid IPv6 address of the destination host.
- `hostname`—Hostname of the destination host. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, `console(config)#snmp-server host "host name"

- `initTtl`—The initial time-to-live (TTL); the maximum number of router hops between the local and remote system (Range: 1–255). The default is 1.
- `maxTtl`—The largest TTL value that can be used (Range: 1–255). This must be larger or equal to the value specified in `initTtl`.
- `maxFail`—Terminate the traceroute after failing to receive a response for this number of consecutive probes (Range: 1–255).
- `interval`—The timeout period. If a response is not received within this period of time, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe, then it sends the next probe immediately. (Range: 1–60 seconds). The default is 3.
- `count`—The number of probes to be sent at each TTL level (Range: 1–10).
- `port`—The destination UDP port of the probe. This should be an unused port on the remote destination system (Range: 1–65535).
- `size`—The size, in bytes, of the payload of the Echo Requests sent (Range: 0–39936 bytes). The default is 0.
- `src-ip-address`—The IPv4 source address to use in the ICMP echo request packets.
- `vlan-id`—The source VLAN over which to send the echo request.
• loopback-id—A configured loopback ID

Default Configuration
The default count is 3 probes.
The default interval is 3 seconds.
The default size is 0 data bytes.
The default port is 33434.
The default initTtl is 1 hop.
The default maxTtl is 30 hops.
The default maxFail is 5 probes.

Command Mode
Privileged Exec mode

User Guidelines
Traceroute operates by sending a sequence of Internet Control Message Protocol (ICMP) echo request packets. The time-to-live (TTL) value, is used in determining the intermediate routers through which the packet flows toward the destination address. Routers decrement a packet’s TTL value and discard packets whose TTL equals 0. On discarding a packet, the router returns an ICMP time exceeded message to the source. Loopback interfaces are not supported on the N1100-ON Series switches.

Examples
The following example discovers the routes that packets will actually take when traveling to the destination specified in the command.

(console)# traceroute ipv6 2001::2 init-ttl 1 max-ttl 4 max-fail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2, 4 hops max, 43 byte packets:
1 2001::2  708 msec  41 msec  11 msec
2 2001::2  12 msec  13 msec  12 msec
3 2001::2  14 msec  9 msec  11 msec

Command History
Syntax and description updated in 6.4 release.
update bootcode

Use the `update bootcode` command to update the bootcode on one or more switches. For each switch, the bootcode is extracted from the active image and programmed to flash.

**Syntax**

`update bootcode [unit ]`

- `unit` — Unit number.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**User Guidelines**

It is not required to update the boot code unless directed to do so in the release notes. Dell EMC Networking switches utilize a universal boot loader and do not contain version specific dependencies in the boot loader. If unit is not specified, all units in the stack are updated. This command does not reboot the stack members after the update completes. Do not reload or power off stack members during the update process as it may cause a switch to fail on a subsequent boot.

**Example**

The following example updates the bootcode on unit 2.

```
console#update bootcode 2
```
Telnet Server Commands

The Telnet protocol (outlined in RFC 854) allows users (clients) to connect to multiuser computers (servers) on the network. Telnet is often employed when a user communicates with a remote login service.

Telnet is the terminal emulation protocol in the TCP/IP suite. Telnet uses TCP as the transport protocol to initiate a connection between server and client. After connecting, the telnet server and client enter a period of option negotiation that determines the options each side is capable of supporting for the connection. The connected systems can negotiate new options or renegotiate old options at any time. In general, each end of the Telnet connection attempts to implement all options that maximize performance for the systems involved.

When a Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a Network Virtual Terminal, or NVT. Therefore, the server and user hosts do not maintain information about the characteristics of each other's terminals and terminal-handling conventions.

Telnet Client Behaviors

Different telnet clients operate differently with respect to the display of the login banner, the MOTD banner and acknowledgments. The following behaviors have been observed for some widely used telnet clients with a MOTD banner configured with the following text:

If you need to utilize this device or otherwise make changes to the configuration, you may contact the owner at x38525.

Please, be advised this unit is under test.

and a login banner configured with the following text:

Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.

Examples

1  SSH (putty):

login as: dellradius
If you need to utilize this device or otherwise make changes to the configuration, you may contact the owner at x38525.
Please, be advised this unit is under test.
dellradius@192.168.12.84's password:

Press 'y' to continue (within 30 seconds) (y/n)
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.

2  SSH (Linux Terminal):

[root ~]# ssh 192.168.12.84 -l dellradius
If you need to utilize this device or otherwise make changes to the configuration, you may contact the owner at x38525.
Please, be advised this unit is under test.
dellradius@192.168.12.84's password:

Press 'y' to continue (within 30 seconds) (y/n)
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.

3  SSH (xterm):

[root ~]# ssh 192.168.12.84 -l dellradius
If you need to utilize this device or otherwise make changes to the configuration, you may contact the owner at x38525.
Please, be advised this unit is under test.
dellradius@192.168.12.84's password:

Press 'y' to continue (within 30 seconds) (y/n)
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.

4  Telnet:

If you need to utilize this device or otherwise make changes to the configuration, you may contact the owner at x38525.
Press 'y' to continue (within 30 seconds) (y/n) y

Please, be advised this unit is under test.
User:root
Password:******
Welcome to the N3024 in the Bottom Chassis - 192.168.12.190. This unit is located in A2 and is currently under test.
**Command History**

Examples updated in 6.4 release.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip telnet server disable</code></td>
<td>The ip telnet server disable command is used to enable/disable the Telnet service on the switch.</td>
</tr>
<tr>
<td><code>ip telnet port</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip telnet</code></td>
<td></td>
</tr>
</tbody>
</table>

**ip telnet server disable**

The ip telnet server disable command is used to enable/disable the Telnet service on the switch.

**Syntax**

`ip telnet server disable`

`no ip telnet server disable`

**Command Mode**

Global Configuration

**User Guidelines**

No specific guidelines.

**Default Value**

This feature is enabled by default.

Dell EMC Networking N-Series switches support the Telnet service over IPv4 and IPv6.

**Example**

```console
console#configure
console(config)#ip telnet server disable
console(config)# no ip telnet server disable
```
**ip telnet port**

The `ip telnet port` command is used to configure the Telnet TCP port number on which the switch listens for Telnet connections.

**Syntax**

```
ip telnet port port number
```

- `port number` — Telnet TCP port number (Range: 1025–65535)

**Default Configuration**

The default value for the Telnet TCP port is 23.

**Command Mode**

Global Configuration

**User Guidelines**

The Telnet server TCP port should not be set to a value that might conflict with other well-known protocol port numbers used on this switch.

UDP, TCP and RAW ports reserved by the switch and unavailable for use or configuration are:

Ports 1, 17, 58, 255, 546, 547, 2222, 4567, 6343, 49160

**Example**

```
console(config)#ip telnet port 1045
console(config)#no ip telnet port
```

**show ip telnet**

The `show ip telnet` command displays the status of the Telnet server and the Telnet TCP port number.

**Syntax**

```
show ip telnet
```

**Default Configuration**

This command has no default configuration.
**Command Mode**

Privileged Exec, Global Configuration mode and all Configuration submodes

**Example**

```
console#show ip telnet
Telnet Server is Enabled. Port:23
```
Time Ranges Commands

Time ranges are used with time-based ACLs to restrict their application due to specific time slots.

This section explains the following commands:

<table>
<thead>
<tr>
<th>time-range [name]</th>
<th>periodic</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute show time-range</td>
<td></td>
</tr>
</tbody>
</table>

**time-range [name]**

Use the `time-range` command to globally enable or disable the event notification service of the time range component. If disabled, ACLs using time ranges are not started.

Use the optional name parameter to create a time range consisting of one absolute time entry and/or one or more periodic time entries. If a time range by this name already exists, this command enters Time-Range Configuration mode to allow updating the time range entries.

Use the `no` form of the command to disable the event notification service.

Use the `no` form of this command with the optional name parameter to delete a time-range identified by name.

**Syntax**

- `time-range [name]`
- `no time-range [name]`

  - name—A case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

**Default Configuration**

Time range event notification is enabled by default.
**Command Mode**
Global Configuration

**User Guidelines**
The CLI mode changes to Time-Range Configuration mode when you successfully execute this command.

**Example**
```
console(config)#time-range timeRange_1
```

**absolute**
Use the absolute command in Time Range Configuration mode to add an absolute time entry to a time range.
Use the **no** form of this command to delete the absolute time entry in the time range.

**Syntax**
```
absolute { [start time date] [end time date] }
no absolute
```
- **start** time date—Time and date at which the configuration that referenced the time range is in effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.
- **end** time date—Time and date at which the configuration that referenced the time range is no longer in effect. Same time and date format as described for the start. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

**Default Configuration**
This command has no default configuration.
**Command Mode**
Time Range Configuration

**User Guidelines**
Only one absolute time entry is allowed per time-range. The time parameter is referenced to the currently configured time zone.

**Example**
```
console#time-range timeRange_1
console(config-time-range)#absolute end 12:00 16 Dec 2010
```

**periodic**
Use the periodic command to add a periodic time entry to a time range. The time parameter is based off of the currently configured time zone. Use the `no` form of this command to delete a periodic time entry from a time-range.

**Syntax**
```
periodic {days-of-the-week  time} to { [days-of-the-week] time }
no periodic
```
- `days-of-the-week`—The first occurrence of this argument is the starting day or days from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted.
  
  This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.

  Other possible values are:
  - daily -- Monday through Sunday
  - weekdays -- Monday through Friday
  - weekend -- Saturday and Sunday
  - If the ending days of the week are the same as the starting days of the week, they can be omitted.
- **time**—The first occurrence of this argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

  The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Time Range Configuration

**User Guidelines**

Multiple periodic entries can exist in a time range, but periodic time entries cannot overlap each other. Periodic time entries can also coexist with an absolute time entry in a time range.

When both periodic and absolute time entries are specified within a time range, the periodic time entries limit the time range to only those times specified within the periodic time range and bounded by the absolute time range. In this case, the absolute time entry specifies the absolute start and end dates/times and the periodic entries specify the start/stop times within the limits of the absolute time entry dates and times.

If a periodic time entry is added to an active time-range with an existing absolute time entry, the absolute time entry immediately becomes inactive. For example, an administrator applies a absolute time-range configured for a week's work hours (08/09-08/13 9am to 6pm) and later adds multiple periodic entries for same days configured individually (Monday, Tuesday, Wednesday, Thursday, Friday) but with after-work hours (9pm to 11pm). The administrator wants to permit/deny HTTP traffic for this time-range, but the entire time-range is invalid due to conflicting entries. The absolute entry is forced to inactive because the periodic entry time is not yet in effect.

**Examples**

```
console#time-range timeRange_2
console(config-time-range)#periodic monday 00:00 to tuesday 12:30
```
console(config-time-range)#periodic tuesday 13:00 to wednesday 12:00
console(config-time-range)#periodic wednesday 12:30 to thursday 20:00
console(config-time-range)#periodic weekend 18:00 to 20:00

**show time-range**

Use the show time-range command to display a time range and all the absolute/periodic time entries that are defined for the time range. The [name] parameter is used to identify a specific time range to display. When the [name] parameter is not specified, all the time ranges defined in the system are displayed.

**Syntax**

```
show time-range [name]
```

- **name**—A specific time range to display

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command outputs the following.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Time Ranges</td>
<td>Number of time ranges configured in the system.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Name of the time range.</td>
</tr>
<tr>
<td>Time Range Status</td>
<td>Status of the time range (active/inactive).</td>
</tr>
<tr>
<td>Absolute start</td>
<td>Start time and day for absolute time entry.</td>
</tr>
<tr>
<td>Absolute end</td>
<td>End time and day for absolute time entry.</td>
</tr>
<tr>
<td>Periodic Entries</td>
<td>Number of periodic entries in a time-range.</td>
</tr>
</tbody>
</table>
### Examples

```console
console#show time-range
```

Admin mode: Enabled  
Current number of all Time Ranges: 1  
Maximum number of all Time Ranges: 100

<table>
<thead>
<tr>
<th>Time Range Name</th>
<th>Status</th>
<th>Entry count</th>
<th>Absolute Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1</td>
<td>Active</td>
<td>0</td>
<td>Does not exist</td>
</tr>
</tbody>
</table>

**Parameter** | **Description**  
--- | ---  
Periodic start | Start time and day for periodic entry.  
Periodic end | End time and day for periodic entry.
USB Flash Drive Commands

When available, a USB flash drive can be used to configure, upgrade and provide consistency to a switching network. A USB flash drive can be plugged in sequentially to a set of routers/switches to upgrade to newer software versions without depending on the network to upgrade the switches with new firmware. New switches can be preloaded with configuration prior to deployment.

The USB Configuration Port provides access to an optional secondary storage capability to the switch. A USB flash drive can be used to store and deploy configurations and images from USB flash drive to the switch. A USB flash drive can be used easily to move and copy configuration and image files from one switch to other. Files from the switch can be copied to a USB flash device and can be used to deploy on other switches in the network.

Validation of Files Downloaded/Uploaded from USB Device

Image files are validated before downloading from the USB flash drive to the switch. Files other than image files and scripts are copied with no validation. Downloaded image files will be validated against the following conditions:

- File exists- Check if the file being downloaded from the USB flash drive exists on the device.
- Valid CRC checksum.- Verify CRC for the file downloaded from the USB flash drive to switch.
- Valid STK format - Check if the file is of type STK.
- Target device validation – Check if the file being downloaded is compatible with the target switch.

Validation for Files Uploaded from Switch to USB Flash Drive

- Memory insufficient - Check memory availability on the USB flash drive to upload the file.
Files downloaded from USB flash drive are not copied to RAM to perform validations. Instead, the file is directly read from the USB flash device and copied to buffers to perform the necessary validations.

**Downloading and Uploading of Files**

After the file validations are successful, the switch proceeds with downloading of files from the USB flash device to the switch or uploading of files from the switch to the USB flash drive. The status of file download / upload is shown on the console. Detailed messages are logged in the system log for further reference.

**Commands in this Section**

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>unmount usb</td>
<td>unmount usb</td>
</tr>
<tr>
<td>dir usb</td>
<td>dir usb</td>
</tr>
<tr>
<td>show usb</td>
<td>show usb</td>
</tr>
<tr>
<td>recover</td>
<td>recover</td>
</tr>
</tbody>
</table>

**unmount usb**

Use the `unmount usb` command to make the USB flash device inactive.

**Syntax**

`unmount usb`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec

**User Guidelines**

Once a flash drive has been unmounted, it must be removed and reinserted in order to be accessed again. If a file is open on the USB, the unmount will fail. The USB drive can be unmounted after the file operation completes.
Example

```
console#unmount usb
```

**Command History**

Description updated in 6.4 release.

**show usb**

Use the `show usb` command to display the USB flash device details.

**Syntax**

```
show usb device
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec

**User Guidelines**

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Status</td>
<td>This field specifies the current status of device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong> if device is plugged-in and the device is recognized by the</td>
</tr>
<tr>
<td></td>
<td>switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inactive</strong> if device is not mounted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid</strong> if device is not present or invalid device is plugged-in.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Manufacturer details</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the device.</td>
</tr>
<tr>
<td>USB Version</td>
<td>Version of the USB device.</td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
</tr>
<tr>
<td>Class Code</td>
<td>Device Class.</td>
</tr>
<tr>
<td>Subclass Code</td>
<td>Device SubClass.</td>
</tr>
</tbody>
</table>
Example

The following example is the output if the device is plugged into the USB slot.

```console
console#show usb device
Device Status............................... Active
Manufacturer............................... JetFish
Product Name................................ Mass Storage Device
Device Serial Number....................... 4JC25PTQ
Class Code.................................. 0x0000
Subclass Code................................ 0x0000
Protocol..................................... 0x0000
Vendor ID.................................... 0x8564
Product ID................................... 0x1000
USB Version Compliance...................... 2.0
```

The following example is the output if the device is not plugged into the USB slot.

```console
console#show usb device
USB flash device is not plugged in.
```

**dir usb**

Use the `dir usb` command to display the USB device contents and memory statistics.

**Syntax**

```
dir usb [subdir]
```

- A subdirectory that exists on the USB flash drive. Multiple levels of subdirectories may be specified in a single string using the forward slash (/) path separator.
Default Configuration
This command has no default configuration.

Command Mode
Privileged Exec

User Guidelines
Only the first 32 characters of the file name are displayed, even if the file name is longer.

Examples

console#dir usb

<table>
<thead>
<tr>
<th>Attr</th>
<th>Size(bytes)</th>
<th>Creation Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwx</td>
<td>2640</td>
<td>Feb 02 2022 00:26:43</td>
<td>.</td>
</tr>
<tr>
<td>drwx</td>
<td>0</td>
<td>Feb 19 2014 15:22:53</td>
<td>..</td>
</tr>
<tr>
<td>-rw-</td>
<td>96</td>
<td>Jan 28 2022 23:05:45</td>
<td>snmpOprData.cfg</td>
</tr>
<tr>
<td>-rw-</td>
<td>14363703</td>
<td>Jan 22 2022 03:36:08</td>
<td>image1.stk</td>
</tr>
</tbody>
</table>

Total Size: 1001914368
Bytes Used: 128319488
Bytes Free: 873594880

console#dir usb examples

<table>
<thead>
<tr>
<th>Attr</th>
<th>Size(bytes)</th>
<th>Creation Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwx</td>
<td>1024</td>
<td>Feb 02 2022 00:26:43</td>
<td>.</td>
</tr>
<tr>
<td>drwx</td>
<td>0</td>
<td>Feb 19 2014 15:22:53</td>
<td>..</td>
</tr>
<tr>
<td>-rw-</td>
<td>96</td>
<td>Jan 28 2022 23:05:45</td>
<td>examples/example.txt</td>
</tr>
</tbody>
</table>

Total Size: 1001914368
Bytes Used: 128319488
Bytes Free: 873594880

console#dir usb examples/..}

<table>
<thead>
<tr>
<th>Attr</th>
<th>Size(bytes)</th>
<th>Creation Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwx</td>
<td>2640</td>
<td>Feb 02 2022 00:26:43</td>
<td>.</td>
</tr>
<tr>
<td>drwx</td>
<td>0</td>
<td>Feb 19 2014 15:22:53</td>
<td>..</td>
</tr>
<tr>
<td>-rw-</td>
<td>96</td>
<td>Jan 28 2022 23:05:45</td>
<td>examples/../snmpOprData.cfg</td>
</tr>
<tr>
<td>-rw-</td>
<td>14363703</td>
<td>Jan 22 2022 03:36:08</td>
<td>examples/../image1.stk</td>
</tr>
</tbody>
</table>
recover

The recover command is implemented as a u-boot environment variable. It mounts the USB stick, copies the image from the USB root level directory into RAM, and executes the image.

Syntax

recover <image-name>

- image-name—The name of a valid firmware stack file located in the root of the mounted USB stick.

Default Configuration

This command has no default configuration.

Command Mode

u-boot mode

User Guidelines

There is no validation of the image.

There is no validation that the image exists on the USB stick (other than the copy fails). Incorrect use of this capability can stop a switch. Stopped switches are not recoverable. Recovery of the switch from the booted image is as needed. No guidelines are provided.
User Interface Commands

This section explains the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Use the configure terminal command to enter Global Configuration mode. This command is equivalent to the configure command with no terminal argument.</td>
</tr>
<tr>
<td>do</td>
<td>Use the do command to execute commands available in Privileged Exec mode from Global Configuration or any Configuration submode with command line completion.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>quit</td>
<td></td>
</tr>
</tbody>
</table>

**configure terminal**

Use the configure terminal command to enter Global Configuration mode. This command is equivalent to the configure command with no terminal argument.

**Syntax**

configure [terminal]

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged Exec mode

**Example**

```console
console#conf t
console(config)#

console#configure terminal
console(config)#
```

**do**

Use the do command to execute commands available in Privileged Exec mode from Global Configuration or any Configuration submode with command line completion.
Syntax

do line

do ?

- line — Command to be executed. It must be an unambiguous command from the Privileged Exec mode. Commands such as configure are forbidden. Command line completion for the line parameter is supported. Users may only execute commands for which they have the appropriate privileges.

Default Configuration

This command has no default configuration.

Command Mode

All modes except Privileged Exec and User Exec modes.

User Guidelines

Command completion using the space bar is available when using this command.

Example #1

crash>
en
console#configure
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#d?
description              dhcp                     do
dot1x                    duplex

console(config-if-Gi1/0/1)#do ?     ! Help from privileged Exec level

console(config-if-Gi1/0/1)#do ?

application Start or stop an application.
arp Purge a dynamic or gateway ARP entry.
boot Select a boot image for use on the next reload.
captive-portal Manage captive portal clients.
clear Clear learned configuration or statistics.
configure Enter global config mode.
connect Connect console session to another stack unit.
copy Copy files to or from the switch.
debug Configure debug flags.
delete Delete a file.
dir                      Display directory information.
disconnect              Close remote console session(s).
dot1x                    Initialize dot1x or reauthenticate clients.
enable                  Enter into user privilege mode.
erase                   Delete a file.
exit                     Exit privileged exec mode.
filedescr                Set a text description for an image file.
help                     Display help for various special keys.
locate                  Blink the locator LED.
logout                  Exit this session. Any unsaved changes are lost.
monitor                 Configure packet monitoring.
ping                    Send ICMP echo packets to a specified IP address.
quit                     Exit this session. Any unsaved changes are lost.
release                 Release an in-band DHCP assigned address.
reload                  Reload stack or a switch in the stack.
rename                  Rename a file.
renew                   Renew an in-band DHCP assigned address.
script                  Manage and execute configuration scripts.
show                    Show configured settings and operational status.
telnet                  Open a telnet connection to another system.
terminal                Configure console session parameters.
test                    Test a copper port. Disable EEE modes first!
traceroute              Trace route to destination.
udld                    Reset UDLD disabled interfaces.
unmount                 Flush cache and un-mount a USB device.
write                   Copy running configuration to startup configuration.

console(config-if-Gil/0/1)#do a?

application        arp

**enable**

Use the `enable` command in User Exec mode to enter the Privileged Exec mode.

**Syntax**

`enable`

**Default Configuration**

The default privilege level is 15.
**Command Mode**
User Exec and Privileged Exec modes

**User Guidelines**
If there is no authentication method defined for enable, then a privilege level 1 user is not allowed to execute this command.

**Example**
The following example shows how to enter privileged mode.

```
console>enable
console#
```

**end**
Use the `end` command to return the CLI command mode back to the privileged execution mode or user execution mode.

**Syntax**
end

**Default Configuration**
This command has no default configuration.

**Command Mode**
All command modes

**User Guidelines**
The first invocation of `end` from Global Configuration mode, or any configuration submode, returns the command mode to Privileged Exec mode. This command is equivalent to using the Ctrl-Z key press.

**Example**
```
console(config)#end
console#end
console>
```
exit
Use the exit command to go to the next lower command mode or, in User Exec mode, to close an active terminal session by logging off the switch.

Syntax
exit

Default Configuration
This command has no default configuration.

Command Mode
All command modes. In User Exec mode, this command behaves identically to the quit command.

User Guidelines
There are no user guidelines for this command.

Example
The following example changes the configuration mode from Interface Configuration mode to User Exec mode to the login prompt.

```
console(config-if-Gi1/0/1)# exit
console(config)# exit
console#exit
console>exit

User:
```

quit
Use the quit command in User Exec mode to close an active terminal session by logging off the switch.

Syntax
quit
**Default Configuration**
This command has no default configuration.

**Command Mode**
User Exec command mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example closes an active terminal session.

```
console>quit
```
Web Server Commands

If enabled, the Dell EMC Networking is manageable via industry standard web browsers. User privilege levels are the same as for the CLI. Over 95% of the management functions are available via the web interface, including configuration and firmware upgrades.

Web Sessions

The HTTP protocol does not provide support for persistent connections. Connections are constantly made and broken so there is no way to know who is accessing the web interface or for how long they are doing so. Additionally, with the use of basic authentication the user authorization is handled by the client browser. This means that once entered, the user name and password are cached in the browser and given to the server on request. Effectively, once a user logs in to the switch, they have access until the browser closes, even across reboots of the switch. This poses a security threat.

The Web Sessions feature makes use of cookies to control web connections, sessions. Cookies must be enabled on the browser. The Set-Cookie directive is sent only once at initiation of the session. With the introduction of Web Sessions the client connections can be monitored and controlled. Web Sessions put the authentication control in the Dell EMC Networking switch instead of the client browser resulting in a more efficient implementation that allows web access while using RADIUS or TACACS+ for authentication. The `exec-timeout` command in line telnet command mode also sets the timeout for the web interface.

The web login is implemented in the login page itself instead of a client browser popup. Additionally, there is a logout button, always present on the web interface. There are various commands that have been modified or added to support Web Sessions. Similarly there are modifications to some of the web pages. Support of SNMP configuration for Web Sessions is also available.

When the authentication method set for web login authentication is set to TACACS+, the exec shell configuration on the TACACS+ server is used to determine user permissions (read-only or read/write). If the configured value on the server is 15, the user is given read-write permissions. Any other value is read-only. If exec shell feature is not enabled on the server, the user is given read-only permissions.
Commands in this Section

This section explains the following commands:

<table>
<thead>
<tr>
<th>common-name</th>
<th>ip http secure-server</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto certificate generate</td>
<td>key-generate</td>
</tr>
<tr>
<td>crypto certificate import</td>
<td>location</td>
</tr>
<tr>
<td>crypto certificate request</td>
<td>no crypto certificate</td>
</tr>
<tr>
<td>duration</td>
<td>organization-unit</td>
</tr>
<tr>
<td>ip http port</td>
<td>show crypto certificate mycertificate</td>
</tr>
<tr>
<td>ip http server</td>
<td>show ip http server status</td>
</tr>
<tr>
<td>ip http secure-certificate</td>
<td>show ip http server secure status</td>
</tr>
<tr>
<td>ip http secure-port</td>
<td>state</td>
</tr>
</tbody>
</table>

common-name

Use the common-name command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the common-name for the switch.

Syntax

common-name common-name

- common-name — Specifies the fully qualified URL or IP address of the switch. If left unspecified, this parameter defaults to the lowest IP address of the switch (when the certificate is generated). (Range: 1–64)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certification mode
**User Guidelines**
This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command.

**Example**
The following example displays how to specify the name of “router.gm.com.”
```
console(config-crypto-cert)#common-name router.gm.com
```

**country**
Use the `country` command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the country.

**Syntax**
```
country country
```
- `country` — Specifies the country name. (Range: 2 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Crypto Certificate Generation or Crypto Certificate Request mode

**User Guidelines**
This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command. The user can enter any two printable characters other than a question mark.

**Example**
The following example displays how to specify the country as “us.”
```
console(config-crypto-cert)#country us
```
crypto certificate generate

Use the crypto certificate generate command to generate a self-signed HTTPS certificate.

Syntax

crypto certificate number generate

• number—Specifies the certificate number. (Range: 1–2)
• generate—Regenerates the SSL RSA key.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command is not saved in the router switch configuration; however, the certificate and keys generated by this command are saved in the private configuration. If the RSA keys do not exist, the generate parameter must be used. The generate sub-command regenerates the RSA key pair. To save the generated certificate and keys on the local switch and distribute the certificate across a stack, save the configuration. Otherwise, the certificate and keys will not be available after the next reboot.

This command generates two files:

• sslt_certN.pem
• sslt_keyN.pem

where N is the certificate number.

To use a signed certificate on the switch, perform the following steps:

• Generate the RSA and DSA keys using the crypto key generate command for RSA followed by DSA.
• Generate a self signed certificate using the crypto key generate command.
• Generate a certificate request using the `crypto certificate request` command. This command uses the DSA keys and the self signed certificate.

• Copy the certificate request displayed on the screen and send it to a CA.

• When the signed certificate is received, copy the signed certificate onto the switch using the `crypto certificate import` command

**Example**

The following example generates a self-signed HTTPS certificate. This certificate can be used to request a certificate from a signing authority.

```
console(config)#crypto certificate 1 generate
console(config-crypto-cert)#common-name DELL
console(config-crypto-cert)#country US
console(config-crypto-cert)#duration 3650
console(config-crypto-cert)#email no-reply@dell.com
console(config-crypto-cert)#location "Round Rock"
console(config-crypto-cert)#organization-name "Dell EMC, Inc."
console(config-crypto-cert)#state TX
console(config-crypto-cert)#key-generate
console(config-crypto-cert)#exit

console(config)#crypto certificate 1 request
console(config-crypto-cert)#common-name DELL
console(config-crypto-cert)#country US
console(config-crypto-cert)#email no-reply@dell.com
console(config-crypto-cert)#location "Round Rock"
console(config-crypto-cert)#organization-name "Dell EMC, Inc."
console(config-crypto-cert)#state TX
console(config-crypto-cert)#key-generate
console(config-crypto-cert)#exit
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB0TCCAToCAQIwgZAxETAPBgNVBAMMCEJST0FEQ09NRcwFQYDVQQKDA5CUkNN
LHU2REV5QJBRDERMA8GA1UECwwIQlJPQURDT00xETAPBgNVBAcMCEJSQ00tSFlE
MQswCQQYDVQQIDA5AJBUDELMAkGA1UEBhMCSU4xIjAgBgkqhkiG9w0BCQEWE3NoeWFt
a0Bicm9hZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADggIBADANBgkqhkiG9w0BAQUF
AAOBgQCd7MvbUt2yb0+piCazzvwyEpfFXZckgY8B9tFaUgxD6plc8xbfRDIKQxor
K85z4bDqogxHDznVx24VTZ4a2JLshGUmUZS4cin2TaqHHi5gI597x5FFYBFTKqS14
YhfgJtA2Bj/W23xmCrIT00ZINIIfwf+PN6cDt2R3ag3hC/+otXw==
```
crypto certificate import

Use the `crypto certificate import` command in Global Configuration mode to import a certificate signed by the Certification Authority for HTTPS.

**Syntax**

crypto certificate number import
  • number — Specifies the certificate number. (Range: 1–2)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command to enter an external certificate (signed by the Certification Authority) to the switch. To end the session, add a period (.) on a separate line after the input, and press ENTER.

The imported certificate must be based on a certificate request created by the `crypto certificate request` Privileged Exec command.

If the public key found in the certificate does not match the switch's SSL RSA key, the command fails.

Regenerating the RSA key will render existing certificates invalid.

Certificates are validated on input. The system log will show any encountered certificate errors such as invalid format or if the certificate could not be validated against the switch private key. Invalid certificates are not imported. The signed certificate must contain the switch public key and match the RSA key on the switch and must be in X509 PEM text format.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration. Certificates are propagated across the stack.
Example

The following example imports a certificate signed by the Certification Authority for HTTPS.

```
console(config)#crypto certificate 1 import

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

-----BEGIN CERTIFICATE-----
MIIDBDCCAewCCC55mFCRMauaDANBgkqhkiG9w0BAQUFADBCTmTEiMKA1UEEwBMCVMx
CzAJBgNVBAgMMAk5DMRAwDgYDVQQHDAdSYWxlaWdoMRUEwYDVQQDDA5EZx
LEElYy4xExARBgNVBAcMCK51dHdvcmtpbmcxGDAWBgNVBAkMD0RIbGwgTmV0d29y
a2luZzEgMB4GCSqGSIb3DQEJARYRbm9yZSBXa1A2GVSbc5j
b20wq28wDQYJKoZIhvcNAQEEBQADgYMQAMIGEwMB4GCSqGSIb3DQEJARYRbm9yZSBXa1A2GVSbc5j
mT+bkg5h0mG2yztCDfu5aWRAIG7yVZjpQU5FwQ/3IJVj6POyMSMC54TXVNV8II
ZHxpdoJ07rewbvvsXpBkzrEWC0zo6w7Ssu0mdgp50zd14c0rRwFyDnBEVxBzG
L4Z8MKT0MQEYgPb+y6FAPgMBAAEwDQYJKoZIhvcNAQETFwQgDgEBAOXM0cZBLMCP
lgf0Jnpv74buMNEqG60oDuAm4E9Pcv76nPvzuarlc87675VpZq297JfWvbBHKA
BY2a2Yo2joGCv7BiIFpoGqbiu+U9w7xwv4j1u+Un8YRshoW7NnNmTnFwTH55SZQ
VFN/UJShWRMvMnOviyzyHaKON+9Fb3rM6CVyiRuWISb31/3LWY9iQJewzoOh
ZK96EgJmznuUjJMoYVhqCE0+LoBWlkhy6ROS+b4cubJpztDtvzn+y8dbM9jSwiky
6FrFVznvamGap8Aw0rUnEV5kMU090hsVU059+QWJwychy9Fhih1hzYzNTprVQs
cPuyXEd8GE=
-----END CERTIFICATE-----
```

Certificate imported successfully

```
console(config)#show crypto certificate mycertificate 1

```

```
-----BEGIN CERTIFICATE-----
MIIDBDCCAewCCC55mFCRMauaDANBgkqhkiG9w0BAQUFADBCTmTEiMKA1UEEwBMCVMx
CzAJBgNVBAgMMAk5DMRAwDgYDVQQHDAdSYWxlaWdoMRUEwYDVQQDDA5EZx
LEElYy4xExARBgNVBAcMCK51dHdvcmtpbmcxGDAWBgNVBAkMD0RIbGwgTmV0d29y
a2luZzEgMB4GCSqGSIb3DQEJARYRbm9yZSBXa1A2GVSbc5j
b20wq28wDQYJKoZIhvcNAQEEBQADgYMQAMIGEwMB4GCSqGSIb3DQEJARYRbm9yZSBXa1A2GVSbc5j
mT+bkg5h0mG2yztCDfu5aWRAIG7yVZjpQU5FwQ/3IJVj6POyMSMC54TXVNV8II
ZHxpdoJ07rewbvvsXpBkzrEWC0zo6w7Ssu0mdgp50zd14c0rRwFyDnBEVxBzG
L4Z8MKT0MQEYgPb+y6FAPgMBAAEwDQYJKoZIhvcNAQETFwQgDgEBAOXM0cZBLMCP
lgf0Jnpv74buMNEqG60oDuAm4E9Pcv76nPvzuarlc87675VpZq297JfWvbBHKA
BY2a2Yo2joGCv7BiIFpoGqbiu+U9w7xwv4j1u+Un8YRshoW7NnNmTnFwTH55SZQ
VFN/UJShWRMvMnOviyzyHaKON+9Fb3rM6CVyiRuWISb31/3LWY9iQJewzoOh
ZK96EgJmznuUjJMoYVhqCE0+LoBWlkhy6ROS+b4cubJpztDtvzn+y8dbM9jSwiky
6FrFVznvamGap8Aw0rUnEV5kMU090hsVU059+QWJwychy9Fhih1hzYzNTprVQs
cPuyXEd8GE=
-----END CERTIFICATE-----
```

Certificate imported successfully

```
```
crypto certificate request

Use the crypto certificate request command to generate and display a certificate request for HTTPS. This command takes you to Crypto Certificate Request mode.

Syntax

crypto certificate number request

  • number — Specifies the certificate number. (Range: 1–2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged Exec mode

User Guidelines

Use this command to generate a certificate request to send to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, you must first generate a self-signed certificate using the crypto certificate generate command in Global Configuration mode in order to sign the certificate request. Make sure to reenter the identical values in the certificate request fields as were entered in the self-signed certificate generated by the crypto certificate generate command.
After receiving the certificate from the Certification Authority, use the `crypto certificate import` command in Global Configuration mode to import the certificate into the switch. This certificate replaces the self-signed certificate. Use the `end` command to exit Crypto Certificate Request mode without generating a certificate request. Use the `exit` command to exit Crypto Certificate Request mode and generate a certificate request.

Example

```bash
console(config)#crypto certificate 1 request
console(config-crypto-cert)#common-name DELL
console(config-crypto-cert)#country US
console(config-crypto-cert)#email no-reply@dell.com
console(config-crypto-cert)#location “Round Rock”
console(config-crypto-cert)#organization-name “Dell EMC”
console(config-crypto-cert)#organization-unit “Dell Networking”
console(config-crypto-cert)#state TX
console(config-crypto-cert)#exit
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBujCCASMCAQIwejENMAsGA1UEAwwEREVTDEYMBYGA1UCwuwPRGVsbCB0ZXZ0MRBj
3Jr7aW5nMRWwEQYDVQQHDHApb3Vu2CBSb2NRnMQswCQYDVQQIDAJUWDELMAkGA1UE
BhMCVVMxIDAeBkgkxkIc9Gw0BCQXEWE5vLXJcGx5QR1bgWuyY29tMIGfMA0GCSqG
SIB3QEBAAUA4GNADCBiQKBgQcb7gWKpCqS5fSx1sWwRygJrU/m5I0YdIhtss
7Qg37uWlkQBv81WY6UFORcEp9yCVY+J0OMjEJAEueE8VTVfNiGR8anaCd63sG77
1z6gVS5M6xFl0HN60s0rLjpnqegQ6eHNXK0cKRWA5wRFQCqYGS+GfDCK9DEBDID2
/sumDwIDAQABQAdABwDQYJKoZIhvcNAQEFBQADgYEaahrQQ/Oi0Gn+R2eQnlyBfwN5
caq=68/GtneLJd0ITQoQhT1NgNDzG0W/TmG2FAumMrP1Xf/bnBhQwCT1MbPE0
HECoTK1AbGhXnSDHfrwvGyH8spWDvCgZ2fsIjY6e4SEE5Lu1J1MRJaLstpZGaQf
mBOBFxspJbh1L+vf=-----END CERTIFICATE REQUEST-----
```

duration

Use the `duration` command in Crypto Certificate Generation mode to specify the duration of certificate validity.

Syntax

duration days

- days — Specifies the number of days a certification would be valid. If left unspecified, the parameter defaults to 365 days. (Range: 30–3650 days)
**Default Configuration**
This command defaults to 365 days.

**Command Mode**
Crypto Certificate Generation mode

**User Guidelines**
This command mode is entered using the `crypto certificate generate` command.

**Example**
The following example displays how specify that a certification is valid for a duration of 50 days.

```
console(config-crypto-cert)#duration 50
```

**ip http port**
Use the `ip http port` command to specify the TCP port on which the switch listens for HTTP connections. To use the default TCP port, use the `no` form of this command.

**Syntax**

```
ip http port port-number
no ip http port
```

- `port-number` — Port number on which the switch HTTP server listens for connections. (Range: 1025–65535)

**Default Configuration**
This default port number is 80.

**Command Mode**
Global Configuration mode
**User Guidelines**

The HTTP TCP port should not be set to a value that might conflict with other well-known protocol port numbers used on this switch.

**Example**

The following example shows how the http port number is configured to 10013.

```plaintext
console(config)#ip http port 10013
```

**ip http server**

Use the `ip http server` command to enable the switch to allow HTTP access to the switch. To disable this function use the `no` form of this command.

**Syntax**

```
ip http server
no ip http server
```

**Default Configuration**

The default mode is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables HTTP access to the switch. Use the `ip http secure-server` command to enable HTTPS access. It is recommended that administrators enable HTTPS access in preference to HTTP access in order to ensure that management activity is not snooped.

**Example**

The following example enables the switch to be configured from a browser.

```plaintext
console(config)#ip http server
```
**ip http secure-certificate**

Use the `ip http secure-certificate` command to configure the active certificate for HTTPS. To return to the default setting, use the no form of this command.

**Syntax**

```
ip http secure-certificate number
no ip http secure-certificate
```

- number—Specifies the certificate number. (Range: 1–2)

**Default Configuration**

The default value of the certificate number is 1.

**Command Mode**

Global Configuration mode

**User Guidelines**

The HTTPS certificate is imported using the `crypto certificate import` command in Global Configuration mode.

**Example**

The following example configures the active certificate for HTTPS.

```console
console(config)#ip http secure-certificate 1
```

**ip http secure-port**

Use the `ip http secure-port` command to configure a TCP port on which the switch listens for HTTPS connections. To use the default port, use the no form of this command.

**Syntax**

```
ip http secure-port port-number
no ip http secure-port
```

```
• port-number—Port number for use by the secure HTTP server. (Range: 1025–65535)

Default Configuration
This default port number is 443.

Command Mode
Global Configuration mode

User Guidelines
The HTTPS TCP port should not be set to a value that might conflict with other well known protocol port numbers used on this switch. It is not possible for the administrator to directly configure the port number to 443 as 443 is out of range. Use the no form of the command to set the port number to the default value of 443.

Example
The following example configures the HTTPS port number to 4545.

```
console(config)#ip http secure-port 4545
```

**ip http secure-server**

Use the `ip http secure-server` command to enable the switch to be accessed via HTTPS clients. To disable HTTPS access, use the `no` form of this command.

**Syntax**

- `ip http secure-server`
- `no ip http secure-server`

**Default Configuration**

The default for the switch is disabled.

**Command Mode**

Global Configuration mode
**User Guidelines**

The switch must be configured with RSA and DSA keys (`crypto key generate`) prior to enabling the HTTP server. Optionally, the switch may be provisioned with up to two signed certificates.

Dell EMC Networking N-Series switches support HTTPS over IPv4 and IPv6.

**Example**

The following example enables the switch to be configured from a browser using HTTPS.

```
console(config)#ip http secure-server
```

**key-generate**

Use the `key-generate` command in Crypto Certificate Generation mode to generate a new RSA key prior to generating the certificate key. The certificate generated by a `crypto certificate generate` command is not a signed certificate and is used to generate a certificate signing request. Once a signed certificate is received, download the certificate to the switch.

**Syntax**

```
key-generate [length]
```

- `length` — Specifies the length of the SSL RSA key. If left unspecified, this parameter defaults to 1024. (Range: 512–2048)

**Default Configuration**

By default, the certificate generation process will utilize existing RSA keys.

**Command Mode**

Crypto Certificate Generation mode

**User Guidelines**

This command mode is entered using the `crypto certificate request` command. You must use the `key-generate` command prior to exiting the crypto certificate request mode to properly generate a certificate request. All
of the common-name, country, location, state, organization-unit, and logging email commands must be issued prior to executing the key-generate command.

**Example**
The following example displays how to specify that you want to regenerate the SSL RSA key 1024 bytes in length.

```
console(config-crypto-cert)#key-generate 1024
```

**location**
Use the `location` command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the location or city name.

**Syntax**
```
location location
```
- location — Specifies the location or city name. (Range: 1–64 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Crypto Certificate Generation or Crypto Certificate Request mode

**User Guidelines**
This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command.

**Example**
The following example displays how to specify the city location of “austin.”

```
console(config-crypto-cert)#location austin
```

**no crypto certificate**
Use the `no crypto certificate` command to delete a certificate.
Syntax

no crypto certificate { openflow | number }

- number—The number of the SSH certificate to remove (between 1 to 2).
- openflow—Remove the openflow certificate and associated information.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The no crypto certificate openflow command erases the Certificate Authority certificates used for validating the OpenFlow Controllers from the switch. Issuing this command automatically disables and re-enables the OpenFlow feature. New SSL certificates may be reloaded from the OpenFlow Controller or may be manually loaded with the copy command.

Example

The following example removes the OpenFlow certificates from the switch and resets the OpenFlow feature.

console(config)#no crypto certificate openflow

organization-unit

Use the organization-unit command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the organization unit.

Syntax

organization-unit organization-unit

- organization-unit — Specifies the organization-unit or department name. (Range: 1–64 characters)
Switch Management Commands

Default Configuration
This command has no default configuration.

Command Mode
Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines
This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command.

Example
The following example displays how to specify the Dell EMC Networking organization-unit.
```
console(config-crypto-cert)#organization-unit "Dell EMC Networking"
```

**show crypto certificate mycertificate**

Use the `show crypto certificate mycertificate` command to view the SSL certificates of your switch.

Syntax
```
show crypto certificate mycertificate [number]
```
- **number** — Specifies the certificate number. (Range: 1–2 digits)

Default configuration
This command has no default configuration.

Command Mode
Privileged Exec mode, Global Configuration mode and all Configuration submodes

Example
The following example displays the SSL certificate of a sample switch.
```
console(config)#show crypto certificate mycertificate 1
```
show ip http server status

Use the show ip http server command to display the HTTP server status information.

Syntax

```
show ip http server status
```

Default Configuration

This command has no default configuration.

Command Mode

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes
**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays the HTTP server configuration.

```
console#show ip http server status
HTTP server enabled. Port: 80
```

**show ip http server secure status**

Use the `show ip http server secure status` command to display the HTTP secure server status information.

**Syntax**

```
show ip http server secure status
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

User Exec mode, Privileged Exec mode, Global Configuration mode and all Configuration submodes

**User Guidelines**

This command has no user guidelines.

**Example**

The following example displays an HTTPS server configuration with DH Key exchange enabled.

```
console#show ip http server secure status
HTTPS server enabled. Port: 443
DH Key exchange enabled.
Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```
The following example displays the HTTPS server configuration with DH Key exchange disabled.

```plaintext
context(config)#show ip http server secure status

HTTPS Server is Disabled. Port: 443
DH Key exchange disabled. Parameters are being generated.
Certificate 1 is active.
Issued by: Dell Networking
Valid from to Oct 22 17:46:02 2017 GMT
Subject: /CN=DELL/OU=Dell Networking/L=Round Rock/ST=TX/C=US/emailAddress=
no-reply@dell.com
Fingerprint: FA06E0DD138FA22A4D696A80171FF3D8
```

**state**

Use the `state` command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the state or province name.

**Syntax**

```plaintext
state state
```

- `state` — Specifies the state or province name. (Range: 1–64 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Crypto Certificate Generation or Crypto Certificate Request mode

**User Guidelines**

This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command.

**Example**

The following example shows how to specify the state of “TX.”

```plaintext
console(config-crypto-cert)#state TX
```
Appendix A: List of Commands

A

aaa accounting .................................................. 867
aaa accounting delay-start .................................. 869
aaa accounting update ....................................... 870
aaa authentication dot1x default ......................... 871
aaa authentication enable ................................ 872
aaa authentication login .................................. 874
aaa authorization ............................................ 876
aaa authorization network default radius ............. 880
aaa ias-user username ..................................... 881
aaa new-model ................................................ 881
aaa server radius dynamic-author ....................... 882
absolute ....................................................... 2305
accounting ................................................... 2022
acct-port ....................................................... 934
action .......................................................... 551
add .............................................................. 553
address-family ............................................... 1258
address-family ipv4 vrf .................................... 1260
address-family ipv6 .......................................... 1261
address-family vpnv4 unicast .............................. 1261
admin-profile ............................................... 910
aggregate-address .......................................... 1263
application install ........................................... 1870
application start ............................................. 1871
application stop ............................................... 1872
area default-cost (Router OSPF) ......................... 1669
area default-cost (Router OSPFv3) ...................... 1757
area nssa (Router OSPF) .................................... 1670
area nssa (Router OSPFv3) ................................ 1758
area nssa default-info-originate (Router OSPF Config) .................................................. 1672
area nssa default-info-originate (Router OSPFv3 Config) .............................................. 1759
area nssa no-redistribute .................................. 1673, 1760
area nssa no-summary ..................................... 1673, 1760
area nssa translator-role ................................ 1674, 1762
area nssa translator-stab-intv ......................... 1675, 1763
area range (Router OSPF) .................................................. 1676
area range (Router OSPFv3) ............................................. 1764
area stub ................................................................. 1678, 1765
area stub no-summary ................................................... 1679, 1766
area virtual-link ......................................................... 1680, 1766
area virtual-link authentication ...................................... 1683
area virtual-link dead-interval ........................................ 1684, 1768
area virtual-link hello-interval ....................................... 1685, 1769
area virtual-link retransmit-interval ............................... 1686, 1770
area virtual-link transmit-delay ..................................... 1687, 1771
arp ................................................................. 1231
arp access-list ........................................................ 378
arp cachesize .......................................................... 1233
arp dynamicrenew ...................................................... 1234
arp purge ............................................................... 1235
arp resptime ........................................................... 1236
arp retries ............................................................... 1237
arp timeout ............................................................. 1237
asset-tag ............................................................... 2210
assign-queue .......................................................... 670
attribute 168 include-in-access-req ................................ 939
attribute 25 ............................................................... 937
attribute 31 ............................................................... 938
attribute 6 ............................................................... 935
attribute 8 ............................................................... 936
authentication enable .................................................. 884
authentication event fail retry ...................................... 940
authentication event server dead action authorize voice ...... 854
authentication order .................................................... 885
authentication priority ................................................ 886
authentication restart .................................................. 887
authentication timeout ................................................ 1032
authorization .......................................................... 2023
auth-port ............................................................... 942
auth-type ............................................................... 1007
auto-cost ............................................................... 1687
automate-tester ......................................................... 943
auto-summary .......................................................... 1821
B

bandwidth ............................................. 1688
banner exec ........................................... 2211
banner login .......................................... 2211
banner motd ........................................... 2212
banner motd acknowledge .............................. 2213
bfd ....................................................... 1689
bfd echo ............................................... 1244
bfd interval .......................................... 1245
bfd slow-timer ......................................... 1247
bgp aggregate-different-meds (BGP Router Configuration) .... 1264
bgp aggregate-different-meds (IPv6 Address Family Configuration) 1265
bgp always-compare-med ............................... 1266
bgp client-to-client reflection (BGP Router Configuration) ........ 1267
bgp client-to-client reflection (IPv6 Address Family Configuration) 1268
bgp cluster-id ......................................... 1269
bgp default local-preference ........................... 1270
bgp fast-external-fallover .............................. 1271
bgp fast-internal-fallover .............................. 1272
bgp listen ............................................... 1273
bgp log-neighbor-changes .............................. 1275
bgp maxas-limit ....................................... 1275
bgp router-id .......................................... 1276
block ..................................................... 1037
boot auto-copy-sw ..................................... 1876
boot auto-copy-sw allow-downgrade ................. 1877
boot host auto-reboot ................................ 1878
boot host auto-save .................................. 1878
boot host dhcp ........................................ 1879
boot host retry-count ................................ 1880
boot system ............................................ 1914
bootfile ................................................. 1944
bootpdhcprelay maxhopcount ......................... 1487
bootpdhcprelay minwaittime ......................... 1488
buffers .................................................. 2215
C

capability opaque ..................................... 1690
captive-portal ........................................ 1032
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal client deauthenticate</td>
<td>1045</td>
</tr>
<tr>
<td>channel-group</td>
<td>631</td>
</tr>
<tr>
<td>class</td>
<td>671</td>
</tr>
<tr>
<td>class-map</td>
<td>672</td>
</tr>
<tr>
<td>class-map rename</td>
<td>674</td>
</tr>
<tr>
<td>classofservice dot1p-mapping</td>
<td>675</td>
</tr>
<tr>
<td>classofservice ip-dscp-mapping</td>
<td>676</td>
</tr>
<tr>
<td>classofservice traffic-class-group</td>
<td>1189</td>
</tr>
<tr>
<td>classofservice trust</td>
<td>679</td>
</tr>
<tr>
<td>clear (IAS)</td>
<td>887</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>1238</td>
</tr>
<tr>
<td>clear arp-cache management</td>
<td>1239</td>
</tr>
<tr>
<td>clear authentication</td>
<td>888</td>
</tr>
<tr>
<td>clear authentication-history</td>
<td>888</td>
</tr>
<tr>
<td>clear authentication statistics</td>
<td>888</td>
</tr>
<tr>
<td>clear captive-portal users</td>
<td>1049</td>
</tr>
<tr>
<td>clear checkpoint statistics</td>
<td>2217</td>
</tr>
<tr>
<td>clear config</td>
<td>1915</td>
</tr>
<tr>
<td>clear counters</td>
<td>390</td>
</tr>
<tr>
<td>clear counters stack-ports</td>
<td>2217</td>
</tr>
<tr>
<td>clear dhcp l2relay statistics interface</td>
<td>342</td>
</tr>
<tr>
<td>clear dot1as statistics</td>
<td>1151</td>
</tr>
<tr>
<td>clear dot1x authentication-history</td>
<td>1024</td>
</tr>
<tr>
<td>clear gmrp statistics</td>
<td>465</td>
</tr>
<tr>
<td>clear green-mode statistics</td>
<td>454</td>
</tr>
<tr>
<td>clear gvrp statistics</td>
<td>467</td>
</tr>
<tr>
<td>clear host</td>
<td>1997</td>
</tr>
<tr>
<td>clear ip address-conflict-detect</td>
<td>1997</td>
</tr>
<tr>
<td>clear ip arp inspection statistics</td>
<td>379</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>1277</td>
</tr>
<tr>
<td>clear ip bgp counters</td>
<td>1279</td>
</tr>
<tr>
<td>clear ip community-list</td>
<td>1448</td>
</tr>
<tr>
<td>clear ip dhcp binding</td>
<td>1944</td>
</tr>
<tr>
<td>clear ip dhcp conflict</td>
<td>1945</td>
</tr>
<tr>
<td>clear ip dhcp snooping binding</td>
<td>345</td>
</tr>
<tr>
<td>clear ip dhcp snooping statistics</td>
<td>346</td>
</tr>
<tr>
<td>clear ip helper statistics</td>
<td>1489</td>
</tr>
<tr>
<td>clear ip mroute</td>
<td>1612</td>
</tr>
<tr>
<td>clear ip ospf</td>
<td>1691</td>
</tr>
<tr>
<td>clear ip ospf configuration</td>
<td>1692</td>
</tr>
</tbody>
</table>
clear ip ospf stub-router ........................................ 1692
clear ip prefix-list ........................................... 1446
clear ipv6 dhcp ................................................... 1968
clear ipv6 dhcp snooping binding .............................. 359
clear ipv6 neighbors .......................................... 1554
clear ipv6 prefix-list ........................................... 1447
clear ipv6 statistics ........................................... 1555
clear isdp counters ............................................ 322
clear isdp table ................................................... 323
clear lldp remote-data ....................................... 557
clear lldp statistics .......................................... 558
clear logging .................................................... 2185
clear logging email statistics ................................ 924
clear logging file .............................................. 2185
clear mac address-table ....................................... 295
clear mmrp statistics ......................................... 1118
clear msrp statistics ......................................... 1132
clear mvrp statistics ......................................... 1125
clear power inline statistics ................................ 2051
clear priority-flow-control statistics ....................... 1223
clear spanning-tree detected-protocols .................... 744
clear vpc statistics ............................................ 589
client .......................................................... 1008
client-identifier ............................................... 1946
client-name ..................................................... 1946
clock set ......................................................... 1902
clock summer-time date .................................... 1905
clock summer-time recurring ............................... 1904
clock timezone hours-offset ................................ 1902
common-name .................................................. 2323
compatible rfc1583 .......................................... 1693
configuration ................................................... 1037
conform-color .................................................. 680
connect .......................................................... 2218
contact-company ............................................... 2172
contact-person .................................................. 2173
controller ....................................................... 1201
copy ............................................................. 1915
cos-queue min-bandwidth .................................... 682
cos-queue random-detect ................................. 684
cos-queue strict ........................................ 686
country .................................................. 2324
crypto certificate generate .............................. 2325
crypto certificate import ................................. 2327
crypto certificate request ............................... 2329
crypto key generate dsa ................................ 1103
crypto key generate rsa ................................ 1104
crypto key pubkey-chain ssh ......................... 1105
crypto key zeroize \{rsa|dsa\} ......................... 1107
crypto key zeroize pubkey-chain ..................... 1106
cut-through mode ...................................... 2219
D
datacenter-bridging .................................... 1180
dcb enable ................................................. 559
deadtime .................................................. 944
debug (HiveAgent) ....................................... 1987
debug aaa accounting .................................. 2076
debug arp .................................................. 2077
debug authentication interface ....................... 2078
debug auto-voip ......................................... 2079
debug bfd ................................................... 2079
debug cfm ................................................ 2080
debug clear ............................................... 2081
debug console ............................................ 2082
debug crashlog .......................................... 2082
debug dhcp packet ....................................... 2085
debug dhcp server packet ............................... 2086
debug dot1ag .............................................. 2087
debug dot1x ............................................... 2088
debug igmpsnooping ................................... 2089
debug ip acl ............................................... 2090
debug ip dvmrp ........................................... 2092
debug ip igmp ............................................. 2093
debug ip mcache ......................................... 2094
debug ip pimdm packet ................................ 2094
debug ip pimsm packet ................................. 2095
debug ipv6 dhcp .......................................... 2096
debug ipv6 mcache ........................................ 2097
debug ipv6 mld .......................................... 2097
debug ipv6 pimdm ....................................... 2098
debug ipv6 pimsm ....................................... 2099
debug isdp ................................................ 2100
debug lacp ............................................... 2101
debug lldp ............................................... 559
debug mldsnooping .................................... 2101
debug ospf .............................................. 2102
debug ospfv3 .......................................... 2103
debug ping ............................................. 2104
debug rip ............................................... 2105
debug sflow ........................................... 2105
debug spanning-tree ................................ 2106
debug udld ............................................. 2107
debug vpc .............................................. 590
debug vrrp ............................................. 2109
default (interface) .................................... 392
default mab ........................................... 992
default metric (BGP Router Configuration) ........ 1281
default metric (IPv6 Address Family Configuration) ..... 1282
default-information originate (BGP Router Configuration) 1279
default-information originate (IPv6 Address Family Configuration) 1280
default-information originate (Router OSPF Configuration) 1693
default-information originate (Router OSPFv3 Configuration) 1771
default-information originate (Router RIP Configuration) 1822
default-metric ....................................... 1695, 1772, 1823
default-router ....................................... 1947
delete .................................................. 1925
delete backup-config ................................ 1926
deny (management) ................................... 1077
deny | permit (IP ACL) ............................... 270
deny | permit (IPv6 ACL) ............................. 508
deny | permit (Mac-Access-List-Configuration) .......... 276
depends-on .......................................... 553
description ......................................... 391, 1847
description (Administrative Profile Config) .......... 911
description (Logging) ................................ 2186
dhcp l2relay (Global Configuration) ............... 333
dhcp l2relay (Interface Configuration) ........................................ 333
dhcp l2relay circuit-id ......................................................... 334
dhcp l2relay remote-id ......................................................... 335
dhcp l2relay trust .............................................................. 335
dhcp l2relay vlan ................................................................. 336
diffserv ................................................................. 687
dir ................................................................. 1926
dir usb ................................................................. 2313
disable ................................................................. 2220
distance ................................................................. 1283
distance bgp (BGP Router Configuration) ............................... 1284
distance bgp (IPv6 Address Family Configuration) ................... 1285
distance ospf ................................................................. 1695, 1773
distance rip ................................................................. 1824
distribute-list out ............................................................. 1696, 1824
distribute-list prefix in ......................................................... 1287
distribute-list prefix out (BGP Router Configuration mode) ....... 1287
distribute-list prefix out (IPv6 Address Family Configuration) ... 1288
dns-server (IP DHCP Pool Config) ........................................ 1948
dns-server (IPv6 DHCP Pool Config) ....................................... 1969
do ................................................................. 2316
domain-name (IP DHCP Pool Config) ..................................... 1949
domain-name (IPv6 DHCP Pool Config) ................................... 1969
dos-control firstfrag ......................................................... 1063
dos-control icmp ............................................................... 1063
dos-control ipv4port ......................................................... 1064
dos-control ipstdip ............................................................. 1065
dos-control tcpflag ............................................................ 1066
dos-control tcpfrag ............................................................ 1066
dot1as (Global Configuration) ............................................. 1152
dot1as (Interface Configuration) .............................................. 1153
dot1as interval announce ...................................................... 1155
dot1as interval pdelay ......................................................... 1158
dot1as interval pdelay-loss .................................................. 1163
dot1as interval sync ............................................................ 1157
dot1as pdelay-threshold ...................................................... 1162
dot1as priority ................................................................. 1154
dot1as timeout announce ..................................................... 1159
dot1as timeout sync ........................................................... 1161
dot1x dynamic-vlan enable ........................................ 989
dot1x guest-vlan ..................................................... 1025
dot1x initialize ....................................................... 991
dot1x max-reauth-req ............................................... 995
dot1x max-req ......................................................... 996
dot1x max-users ....................................................... 997
dot1x port-control .................................................... 998
dot1x re-authenticate ............................................... 999
dot1x reauthentication ............................................. 1000
dot1x system-auth-control ......................................... 1001
dot1x system-auth-control monitor ................................ 1002
dot1x timeout guest-vlan-period .................................. 1026
dot1x timeout quiet-period ......................................... 1003
dot1x timeout re-authperiod ....................................... 1004
dot1x timeout server-timeout ....................................... 1005
dot1x timeout tx-period ............................................ 1006
dot1x unauth-vlan .................................................... 1027
drop ................................................................. 688
duplex ............................................................... 393
duration ............................................................. 2330

E
enable .......................................................... 1033, 1038, 1289, 1697, 1774, 1825, 1888, 2318
enable authentication ............................................. 2024
enable password ..................................................... 889
enable password encrypted ....................................... 1099
encapsulation ........................................................ 1505
end ................................................................. 2319
erase ............................................................... 1927
errdisable recovery cause ......................................... 499
erddisable recovery interval ....................................... 501
ethernet cfm cc level ............................................... 436
ethernet cfm domain ............................................... 435
ethernet cfm mep active ........................................... 439
ethernet cfm mep archive-hold-time ........................... 439
ethernet cfm mep enable .......................................... 438
ethernet cfm mep level ............................................. 437
ethernet cfm mip level ............................................. 440
eula-consent ......................................................... 1984, 2170
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
<td>346</td>
</tr>
<tr>
<td>ip dhcp snooping binding</td>
<td>347</td>
</tr>
<tr>
<td>ip dhcp snooping database</td>
<td>348</td>
</tr>
<tr>
<td>ip dhcp snooping database write-delay</td>
<td>349</td>
</tr>
<tr>
<td>ip dhcp snooping limit</td>
<td>350</td>
</tr>
<tr>
<td>ip dhcp snooping log-invalid</td>
<td>351</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>352</td>
</tr>
<tr>
<td>ip dhcp snooping verify mac-address</td>
<td>353</td>
</tr>
<tr>
<td>ip domain-lookup</td>
<td>2005</td>
</tr>
<tr>
<td>ip domain-name</td>
<td>2006</td>
</tr>
<tr>
<td>ip dvmrp</td>
<td>1456</td>
</tr>
<tr>
<td>ip dvmrp metric</td>
<td>1457</td>
</tr>
<tr>
<td>ip extcommunity-list</td>
<td>1296</td>
</tr>
<tr>
<td>ip helper enable</td>
<td>1497</td>
</tr>
<tr>
<td>ip helper-address (global configuration)</td>
<td>1493</td>
</tr>
<tr>
<td>ip helper-address (interface configuration)</td>
<td>1495</td>
</tr>
<tr>
<td>ip host</td>
<td>2007</td>
</tr>
<tr>
<td>ip http authentication</td>
<td>890</td>
</tr>
<tr>
<td>ip http port</td>
<td>2331</td>
</tr>
<tr>
<td>ip http secure-certificate</td>
<td>2333</td>
</tr>
<tr>
<td>ip http secure-port</td>
<td>2333</td>
</tr>
<tr>
<td>ip http secure-server</td>
<td>2334</td>
</tr>
<tr>
<td>ip http server</td>
<td>2332</td>
</tr>
<tr>
<td>ip http timeout policy</td>
<td>2115</td>
</tr>
<tr>
<td>ip https authentication</td>
<td>891</td>
</tr>
<tr>
<td>ip icmp echo-reply</td>
<td>1505</td>
</tr>
<tr>
<td>ip icmp error-interval</td>
<td>1506</td>
</tr>
<tr>
<td>ip igmp last-member-query-count</td>
<td>1464</td>
</tr>
<tr>
<td>ip igmp last-member-query-interval</td>
<td>1465</td>
</tr>
<tr>
<td>ip igmp mroute-proxy</td>
<td>1466</td>
</tr>
<tr>
<td>ip igmp proxy-service</td>
<td>1477</td>
</tr>
<tr>
<td>ip igmp proxy-service reset-status</td>
<td>1478</td>
</tr>
<tr>
<td>ip igmp proxy-service unsolicited-report-interval</td>
<td>1479</td>
</tr>
<tr>
<td>ip igmp query-interval</td>
<td>1467</td>
</tr>
<tr>
<td>ip igmp query-max-response-time</td>
<td>1468</td>
</tr>
<tr>
<td>ip igmp robustness</td>
<td>1469</td>
</tr>
<tr>
<td>ip igmp snooping (global)</td>
<td>478</td>
</tr>
<tr>
<td>ip igmp snooping (VLAN)</td>
<td>480</td>
</tr>
<tr>
<td>ip igmp snooping querier</td>
<td>490</td>
</tr>
</tbody>
</table>
ip igmp snooping querier election participate ................. 492
ip igmp snooping querier query-interval ....................... 493
ip igmp snooping querier timer expiry .......................... 494
ip igmp snooping querier version ............................... 495
ip igmp snooping report-suppression ............................ 487
ip igmp snooping unregistered floodall ......................... 487
ip igmp snooping vlan groupmembership-interval ............... 484
ip igmp snooping vlan immediate-leave ......................... 483
ip igmp snooping vlan last-member-query-interval ............. 485
ip igmp snooping vlan mrouter .................................. 488
ip igmp startup-query-count .................................... 1469
ip igmp startup-query-interval .................................. 1470
ip igmp version .................................................. 1471
ip irdp .......................................................... 1813
ip irdp holdtime ............................................... 1815
ip irdp maxadvertinterval ......................................... 1816
ip irdp minadvertinterval ......................................... 1817
ip irdp multicast ................................................ 1818
ip irdp preference .............................................. 1818
ip local-proxy-arp .............................................. 1240
ip mroute ......................................................... 1614
ip multicast boundary ............................................. 1614
ip multicast ttl-threshold ........................................ 1617
ip multicast-routing .............................................. 1615
ip name-server ................................................... 2008
ip name-server source-interface .................................. 2008
ip netdirbcast ................................................... 1507
ip ospf area ....................................................... 1700
ip ospf authentication ............................................ 1701
ip ospf bfd ......................................................... 1248
ip ospf cost ........................................................ 1702
ip ospf database-filter all out ................................... 1702
ip ospf dead-interval ............................................. 1703
ip ospf hello-interval ............................................. 1704
ip ospf mtu-ignore ............................................... 1704
ip ospf network .................................................. 1705
ip ospf priority .................................................... 1706
ip ospf retransmit-interval ....................................... 1707
ipv6 nd managed-config-flag ........................................ 1566
ipv6 nd ns-interval .................................................. 1567
ipv6 nd nud max-multicast-solicits ................................. 1568
ipv6 nd nud max-unicast-solicits ................................. 1569
ipv6 nd nud retry .................................................... 1570
ipv6 nd other-config-flag ........................................... 1571
ipv6 nd prefix ......................................................... 1572
ipv6 nd ra hop-limit unspecified .................................. 1566
ipv6 nd raguard attach-policy ..................................... 1573
ipv6 nd ra-interval ................................................... 1574
ipv6 nd ra-lifetime .................................................... 1575
ipv6 nd reachable-time ................................................ 1576
ipv6 nd suppress-ra ................................................. 1577
ipv6 ospf ................................................................. 1776
ipv6 ospf area ......................................................... 1777
ipv6 ospf bfd .......................................................... 1249
ipv6 ospf cost .......................................................... 1778
ipv6 ospf dead-interval ............................................. 1779
ipv6 ospf hello-interval ............................................. 1779
ipv6 ospf mtu-ignore .................................................. 1780
ipv6 ospf network ..................................................... 1781
ipv6 ospf priority ........................................................ 1782
ipv6 ospf retransmit-interval ..................................... 1783
ipv6 ospf transmit-delay ............................................ 1784
ipv6 pim (VLAN Interface config) ................................. 1643
ipv6 pim bsr-border .................................................. 1644
ipv6 pim bsr-candidate ............................................. 1645
ipv6 pim dense-mode .................................................. 1646
ipv6 pim dr-priority ................................................... 1646
ipv6 pim hello-interval ............................................. 1647
ipv6 pim join-prune-interval ..................................... 1648
ipv6 pim register-threshold ....................................... 1648
ipv6 pim rp-address .................................................. 1649
ipv6 pim rp-candidate ................................................. 1650
ipv6 pim sparse-mode ................................................. 1651
ipv6 pim ssm ............................................................. 1652
ipv6 prefix-list ........................................................ 1433
ipv6 redirect .......................................................... 1577
ipv6 route ............................................................... 1578
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 route distance</td>
<td>1580</td>
</tr>
<tr>
<td>ipv6 router ospf</td>
<td>1784</td>
</tr>
<tr>
<td>ipv6 traffic-filter</td>
<td>516</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>1581</td>
</tr>
<tr>
<td>ipv6 unreachables</td>
<td>1581</td>
</tr>
<tr>
<td>ipv6 verify binding</td>
<td>368</td>
</tr>
<tr>
<td>ipv6 verify source</td>
<td>369, 1455, 1983</td>
</tr>
<tr>
<td>iscsi aging time</td>
<td>546</td>
</tr>
<tr>
<td>iscsi cos</td>
<td>546</td>
</tr>
<tr>
<td>iscsi enable</td>
<td>548</td>
</tr>
<tr>
<td>iscsi target port</td>
<td>549</td>
</tr>
<tr>
<td>isdp advertise-v2</td>
<td>323</td>
</tr>
<tr>
<td>isdp enable</td>
<td>324</td>
</tr>
<tr>
<td>isdp holdtime</td>
<td>325</td>
</tr>
<tr>
<td>isdp timer</td>
<td>326</td>
</tr>
<tr>
<td>keepalive (Global Config)</td>
<td>584</td>
</tr>
<tr>
<td>keepalive (Interface Config)</td>
<td>582</td>
</tr>
<tr>
<td>keepalive action</td>
<td>585</td>
</tr>
<tr>
<td>key</td>
<td>945, 978</td>
</tr>
<tr>
<td>key-generate</td>
<td>2335</td>
</tr>
<tr>
<td>key-string</td>
<td>1111</td>
</tr>
<tr>
<td>lacp port-priority</td>
<td>635</td>
</tr>
<tr>
<td>lacp system-priority</td>
<td>636</td>
</tr>
<tr>
<td>lacp timeout</td>
<td>637</td>
</tr>
<tr>
<td>lease</td>
<td>1954</td>
</tr>
<tr>
<td>level</td>
<td>2187</td>
</tr>
<tr>
<td>line</td>
<td>2028</td>
</tr>
<tr>
<td>link debounce time</td>
<td>398</td>
</tr>
<tr>
<td>link-dependency group</td>
<td>552</td>
</tr>
<tr>
<td>lldp dcbx port-role</td>
<td>1182</td>
</tr>
<tr>
<td>lldp dcbx version</td>
<td>1181</td>
</tr>
<tr>
<td>lldp med</td>
<td>560</td>
</tr>
<tr>
<td>lldp med confignotification</td>
<td>561</td>
</tr>
<tr>
<td>lldp med faststartrepeatcount</td>
<td>561</td>
</tr>
<tr>
<td>lldp med transmit-tlv</td>
<td>562</td>
</tr>
<tr>
<td>lldp notification</td>
<td>563</td>
</tr>
</tbody>
</table>
mac access-list extended ................................................ 283
mac access-list extended rename .................................. 283
mac address-table aging-time ....................................... 296
mac address-table multicast forbidden address ............... 297
mac address-table static ............................................. 298
macro apply .............................................................. 1888
macro description ...................................................... 1889
macro global apply .................................................... 1886
macro global description ............................................ 1887
macro global trace ..................................................... 1886
macro name .............................................................. 1884
macro trace .............................................................. 1888
mail-server ip-address | hostname ................................. 925
management access-class ........................................... 1078
management access-list .............................................. 1079
mark cos ................................................................. 689
mark ip-dscp ............................................................ 690
mark ip-precedence .................................................... 691
match access-group ................................................... 692
match any ................................................................. 697
match as-path .......................................................... 1436
match class-map ....................................................... 694
match community ...................................................... 1437
match cos ............................................................... 695
match destination-address mac ..................................... 696
match dstip ............................................................... 698
match dstip6 ............................................................... 699
match dstl4port ........................................................... 700
match ethertype ........................................................... 700
match extcommunity ................................................ 1298
match ip address ....................................................... 1522
match ip address prefix-list ...................................... 1438
match ip dscp ............................................................ 702
match ip precedence .................................................. 703
match ip tos .............................................................. 704
match ip6flowlbl .......................................................... 701
match ipv6 address prefix-list ................................. 1439
match length ............................................................ 1525
match mac-list .......................................................... 1526
mvrp global ............................................................. 1127
mvrp periodic state machine .................................... 1128

N
name (Captive Portal) ............................................... 1041
name (mst) .............................................................. 747
name (RADIUS server) ............................................. 947
name (VLAN Configuration) ........................................ 808
neighbor activate .................................................... 1304
neighbor advertisement-interval (BGP Router Configuration) 1305
neighbor advertisement-interval (IPv6 Address Family Configuration) 1306
neighbor allowas-in .................................................. 1307
neighbor connect-retry-interval ................................... 1309
neighbor default-originate (BGP Router Configuration) ........ 1310
neighbor default-originate (IPv6 Address Family Configuration) 1311
neighbor description ................................................ 1313
neighbor ebgp-multihop ............................................. 1314
neighbor fall-over bfd .............................................. 1250
neighbor filter-list (BGP Router Configuration) ................. 1316
neighbor filter-list (IPv6 Address Family Configuration) ....... 1318
neighbor inherit peer ................................................. 1319
neighbor local-as ..................................................... 1320
neighbor maximum-prefix (BGP Router Configuration) ........... 1322
neighbor maximum-prefix (IPv6 Address Family Configuration) 1324
neighbor next-hop-self (BGP Router Configuration) ............... 1325
neighbor next-hop-self (IPv6 Address Family Configuration) .... 1326
neighbor password .................................................... 1327
neighbor prefix-list (BGP Router Configuration) .................. 1329
neighbor prefix-list (IPv6 Address Family Configuration) ....... 1330
neighbor remote-as .................................................... 1331
neighbor remove-private-as ........................................ 1332
neighbor rfc5549-support .......................................... 1333
neighbor route-map (BGP Router Configuration) .................. 1335
neighbor route-map (IPv6 Address Family Configuration) ....... 1336
neighbor route-reflector-client (BGP Router Configuration) .. 1337
neighbor route-reflector-client (IPv6 Address Family Configuration) 1338
neighbor send-community (BGP Router Configuration) .......... 1340
neighbor send-community IPv6 Address Family Configuration) .. 1341
neighbor shutdown (BGP Router Configuration) ................. 1342
neighbor timers ...................................................... 1343
neighbor update-source ........................................ 1344
netbios-name-server ............................................ 1955
netbios-node-type ................................................ 1956
network ............................................................. 1957
network (BGP Router Configuration) .......................... 1346
network (IPv6 Address Family Configuration) .............. 1348
network area ....................................................... 1712
next-server ......................................................... 1957
no clock summer-time ........................................... 1906
no clock timezone ................................................ 1903
no crypto certificate ............................................. 2336
no priority (management) ........................................ 1081
no user .................................................................. 1050
nsf .................................................................. 1713, 1786, 2230
nsf helper ............................................................ 1714, 1787
nsf helper strict-lsa-checking ................................. 1715, 1788
nsf restart-interval ................................................ 1715, 1788
O
openflow ............................................................. 1208
option .................................................................. 1958
organization-unit ................................................... 2337
P
passive ................................................................. 1209
passive-interface .................................................... 1717, 1789
passive-interface default ......................................... 1716, 1790
password (aaa IAS User Configuration) ...................... 892
password (Line Configuration) ................................. 2031
password (Mail Server Configuration Mode) ............... 928
password (User EXEC) ............................................. 894
passwords aging ..................................................... 1088
passwords history ................................................... 1088
passwords lock-out ................................................ 1089
passwords min-length ............................................. 1090
passwords strength exclude-keyword ......................... 1098
passwords strength max-limit consecutive-characters ..... 1095
passwords strength max-limit repeated-characters ......... 1096
passwords strength minimum character-classes .......... 1097
passwords strength minimum lowercase-letters ........................................ 1093
passwords strength minimum numeric-characters ...................................... 1094
passwords strength minimum special-characters ....................................... 1094
passwords strength minimum uppercase-letters ........................................ 1092
passwords strength-check ................................................................. 1091
peer-detection enable ............................................................................ 591
peer-detection interval ........................................................................... 591
peer-keepalive destination ...................................................................... 592
peer-keepalive enable ............................................................................ 594
peer-keepalive timeout .......................................................................... 595
periodic .................................................................................................... 2306
permit (management) ............................................................................... 1081
permit ip host mac host ........................................................................... 384
ping .......................................................................................................... 2230
ping ethernet cfm .................................................................................... 441
police-simple ........................................................................................... 711
police-single-rate ..................................................................................... 713
police-two-rate ......................................................................................... 714
policy-map ............................................................................................... 716
port ........................................................................................................... 979, 1011, 2203
port (Mail Server Configuration Mode) ..................................................... 926
port-channel local-preference ................................................................... 638
port-channel min-links ............................................................................. 639
power inline .............................................................................................. 2041
power inline detection ............................................................................. 2042
power inline four-pair forced ................................................................... 2043
power inline limit ..................................................................................... 2044
power inline management ....................................................................... 2046
power inline powered-device ................................................................... 2048
power inline priority ................................................................................ 2049
power inline reset .................................................................................... 2049
power inline usage-threshold .................................................................... 2050
prefix-delegation ...................................................................................... 1974
primary ..................................................................................................... 948
priority ...................................................................................................... 949, 980
priority-flow-control mode ..................................................................... 1221
priority-flow-control priority ................................................................... 1222
private-vlan ............................................................................................. 809
process cpu threshold ............................................................................... 2234
<table>
<thead>
<tr>
<th>Command</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>1041</td>
</tr>
<tr>
<td>protocol group</td>
<td>811</td>
</tr>
<tr>
<td>protocol vlan group</td>
<td>812</td>
</tr>
<tr>
<td>protocol vlan group all</td>
<td>813</td>
</tr>
<tr>
<td>protocol-version all</td>
<td>1210</td>
</tr>
<tr>
<td>proxy-ip-address</td>
<td>1989, 2175</td>
</tr>
<tr>
<td>Q</td>
<td>2320</td>
</tr>
<tr>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>radius server</td>
<td>958</td>
</tr>
<tr>
<td>radius server attribute</td>
<td>950</td>
</tr>
<tr>
<td>radius server attribute 168</td>
<td>956</td>
</tr>
<tr>
<td>radius server attribute 168 include-in-access-req</td>
<td>939</td>
</tr>
<tr>
<td>radius server attribute 25</td>
<td>953</td>
</tr>
<tr>
<td>radius server attribute 31</td>
<td>954</td>
</tr>
<tr>
<td>radius server attribute 4</td>
<td>950</td>
</tr>
<tr>
<td>radius server attribute 6</td>
<td>951</td>
</tr>
<tr>
<td>radius server attribute 8</td>
<td>952</td>
</tr>
<tr>
<td>radius server deadtime</td>
<td>957</td>
</tr>
<tr>
<td>radius server key</td>
<td>960</td>
</tr>
<tr>
<td>radius server retransmit</td>
<td>961</td>
</tr>
<tr>
<td>radius server source-interface</td>
<td>963</td>
</tr>
<tr>
<td>radius server source-ip</td>
<td>962</td>
</tr>
<tr>
<td>radius server timeout</td>
<td>964</td>
</tr>
<tr>
<td>radius server vsa send authentication</td>
<td>964</td>
</tr>
<tr>
<td>random-detect exponential-weighting-constant</td>
<td>722</td>
</tr>
<tr>
<td>random-detect queue-parms</td>
<td>717</td>
</tr>
<tr>
<td>rate-limit cpu</td>
<td>1067</td>
</tr>
<tr>
<td>rd</td>
<td>1350</td>
</tr>
<tr>
<td>recover</td>
<td>2315</td>
</tr>
<tr>
<td>redirect</td>
<td>723, 1042</td>
</tr>
<tr>
<td>redirect-url</td>
<td>1042</td>
</tr>
<tr>
<td>redistribute (BGP IPv6)</td>
<td>1353</td>
</tr>
<tr>
<td>redistribute (BGP)</td>
<td>1351</td>
</tr>
<tr>
<td>redistribute (OSPF)</td>
<td>1718</td>
</tr>
<tr>
<td>redistribute (OSPFv3)</td>
<td>1791</td>
</tr>
<tr>
<td>redistribute (RIP)</td>
<td>1830</td>
</tr>
<tr>
<td>release dhcp</td>
<td>1936</td>
</tr>
</tbody>
</table>
reload ................................................................. 2236
remark ............................................................... 284
remote-span ......................................................... 659
rename ............................................................... 1928
renew dhcp .......................................................... 1936
retransmit .......................................................... 967
revision (mst) ....................................................... 748
rmon alarm .......................................................... 2055
rmon collection history .......................................... 2057
rmon event .......................................................... 2058
rmon hcalarm ....................................................... 2059
role priority ......................................................... 596
route-map ........................................................... 1527
router bgp ........................................................... 1257
router ospf .......................................................... 1720
router rip ........................................................... 1831
router-id ............................................................ 1719, 1792
route-target ......................................................... 1355
rule ................................................................. 912
S
script apply ......................................................... 1908
script delete ......................................................... 1909
script list ........................................................... 1910
script show ........................................................ 1910
script validate ..................................................... 1911
security ............................................................. 925
server ............................................................... 1986, 2176
server-key .......................................................... 1012
service ............................................................. 436
service dhcp ......................................................... 1963
service dhcpv6 ...................................................... 1975
service unsupported-transceiver ................................. 2238
service-acl input ................................................... 286
service-policy ....................................................... 724
session-timeout ..................................................... 1043
set as-path .......................................................... 1449
set comm-list delete .............................................. 1450
set community ....................................................... 1451
show bgp ipv6 neighbors ........................................... 1366
show bgp ipv6 neighbors advertised-routes .................... 1372
show bgp ipv6 neighbors policy .................................. 1374
show bgp ipv6 neighbors received-routes ....................... 1375
show bgp ipv6 route-reflection ................................ 1384
show bgp ipv6 statistics .......................................... 1377
show bgp ipv6 summary ........................................... 1378
show bgp ipv6 update-group ...................................... 1381
show boot .......................................................... 1881
show bootvar ....................................................... 1930
show captive-portal .............................................. 1035
show captive-portal client status ................................. 1045
show captive-portal configuration ................................. 1055
show captive-portal configuration client status ............... 1046
show captive-portal configuration interface ................... 1056
show captive-portal configuration locales ....................... 1057
show captive-portal configuration status ....................... 1058
show captive-portal interface client status .................... 1047
show captive-portal interface configuration status .......... 1048
show captive-portal status ....................................... 1036
show captive-portal user ......................................... 1050
show checkpoint statistics ....................................... 2243
show class-map .................................................... 725
show classofservice dot1p-mapping .............................. 726
show classofservice ip-dscp-mapping ............................ 727
show classofservice traffic-class-group ......................... 1196
show classofservice trust ........................................ 729
show cli modes .................................................... 915
show clock ........................................................ 1906
show copper-ports tdr .......................................... 2036
show crypto certificate mycertificate ............................ 2338
show crypto key mypubkey ....................................... 1112
show crypto key pubkey-chain ssh ............................... 1113
show cut-through mode .......................................... 2244
show debugging .................................................... 2116
show dhcp l2relay agent-option vlan ............................ 339
show dhcp l2relay all ............................................ 337
show dhcp l2relay circuit-id vlan ............................... 341
show dhcp l2relay interface .................................... 338
show dhcp l2relay remote-id vlan ........................................... 342
show dhcp l2relay stats interface .......................................... 338
show dhcp l2relay vlan ......................................................... 340
show dhcp lease ................................................................. 1938
show diiffserv ...................................................................... 730
show diiffserv service brief ..................................................... 732
show diiffserv service interface ............................................... 731
show dos-control .................................................................. 1069
show dot1as .......................................................................... 1165
show dot1as statistics ............................................................. 1168
show dot1x ........................................................................... 1014
show dot1x advanced ............................................................. 1028
show dot1x authentication-history ............................................ 1015
show dot1x clients ................................................................. 1017
show dot1x interface ............................................................. 1020
show dot1x interface statistics .................................................. 1022
show dot1x users ................................................................. 1023
show errdisable recovery ........................................................ 502
show ethernet cfm domain ....................................................... 444
show ethernet cfm errors ......................................................... 443
show ethernet cfm maintenance-points local ................................ 445
show ethernet cfm maintenance-points remote ............................ 446
show ethernet cfm statistics .................................................... 447
show eula-consent hiveagent .................................................... 1994
show eula-consent support-assist ............................................. 2177
show exception ..................................................................... 2118
show fiber-ports optical-transceiver .......................................... 2037
show gmrp configuration .......................................................... 465
show green-mode ................................................................ 459
show green-mode eee-lpi-history interface ................................. 461
show green-mode interface-id ................................................... 456
show gvrp configuration .......................................................... 473
show gvrp error-statistics ........................................................ 474
show gvrp statistics ............................................................... 475
show hardware profile ............................................................ 2244
show hiveagent debug ............................................................. 1992
show hiveagent status ............................................................. 1993
show hosts .......................................................................... 2016
show idprom interface ............................................................ 2245
show idprom interface interface-id ................................. 405
show interfaces ............................................... 402, 2246
show interfaces advanced firmware .............................. 2248
show interfaces advertise ........................................ 405
show interfaces configuration ...................................... 406
show interfaces cos-queue ......................................... 733
show interfaces counters .......................................... 407
show interfaces debounce .......................................... 411
show interfaces description ....................................... 412
show interfaces detail ............................................. 413
show interfaces loopback ......................................... 1609
show interfaces port-channel ...................................... 640
show interfaces priority-flow-control ............................ 1224
show interfaces random-detect .................................... 735
show interfaces status ............................................ 414
show interfaces status err-disabled ............................... 504
show interfaces switchport ........................................ 815
show interfaces traffic ............................................ 1197
show interfaces traffic-class-group ............................... 1199
show interfaces transceiver ....................................... 417, 419
show interfaces trunk ............................................ 418
show interfaces tunnel ............................................ 1837
show interfaces utilization ......................................... 2249
show ip access-lists .............................................. 288
show ip address-conflict .......................................... 2017
show ip arp inspection ............................................ 385
show ip arp inspection vlan ....................................... 388
show ip as-path-access-list ....................................... 1440
show ip bgp ..................................................... 1385
show ip bgp aggregate-address .................................... 1387
show ip bgp extcommunity-list ................................... 1390
show ip bgp listen range .......................................... 1391
show ip bgp neighbors ............................................. 1392
show ip bgp neighbors advertised-routes ......................... 1399
show ip bgp neighbors policy ..................................... 1403
show ip bgp neighbors received-routes .......................... 1401
show ip bgp route-reflection ....................................... 1404
show ip bgp statistics ............................................ 1405
show ip bgp summary ............................................. 1407
show ip bgp update-group
show ip bgp vpn4
show ip brief
show ip community-list
show ip dhcp binding
show ip dhcp conflict
show ip dhcp global configuration
show ip dhcp pool
show ip dhcp relay
show ip dhcp server statistics
show ip dhcp snooping
show ip dhcp snooping binding
show ip dhcp snooping database
show ip dhcp snooping interfaces
show ip dhcp snooping statistics
show ip dvmrp
show ip dvmrp interface
show ip dvmrp neighbor
show ip dvmrp nexthop
show ip dvmrp prune
show ip dvmrp route
show ip helper statistics
show ip helper-address
show ip http server secure status
show ip http server status
show ip igmp
show ip igmp groups
show ip igmp interface
show ip igmp interface stats
show ip igmp membership
show ip igmp proxy-service
show ip igmp proxy-service groups
show ip igmp proxy-service groups detail
show ip igmp proxy-service interface
show ip igmp snooping
show ip igmp snooping groups
show ip igmp snooping mrouter
show ip igmp snooping querier
show ip interface
show ip irdp .................................................. 1819
show ip mcast mroute static .............................. 1632
show ip mroute ............................................ 1630
show ip mroute group ...................................... 1631
show ip mroute source .................................... 1631
show ip multicast .......................................... 1628
show ip multicast interface ............................... 1629
show ip ospf ................................................. 1721
show ip ospf abr ........................................... 1727
show ip ospf area .......................................... 1728
show ip ospf asbr .......................................... 1730
show ip ospf database .................................... 1731
show ip ospf database database-summary .............. 1734
show ip ospf interface ..................................... 1736
show ip ospf interface brief .............................. 1738
show ip ospf interface stats .............................. 1739
show ip ospf neighbor ..................................... 1741
show ip ospf range ......................................... 1745
show ip ospf statistics ..................................... 1746
show ip ospf stub table ................................... 1748
show ip ospf traffic ........................................ 1749
show ip ospf virtual-link .................................. 1751
show ip ospf virtual-links brief .......................... 1752
show ip pim .................................................. 1633
show ip pim boundary ...................................... 1628
show ip pim bsr-router .................................... 1634
show ip pim interface ..................................... 1635
show ip pim neighbor ...................................... 1637
show ip pim rp hash ........................................ 1638
show ip pim rp mapping .................................... 1639
show ip pim statistics ..................................... 1640
show ip policy ................................................. 1535
show ip prefix-list ......................................... 1442
show ip protocols .......................................... 1536
show ip rip .................................................... 1832
show ip rip interface ...................................... 1833
show ip rip interface brief ................................ 1834
show ip route ............................................... 1540
show ip route brief ......................................... 1543
show ip route preferences ................................. 1543
show isdp neighbors ............................................................ 329
show isdp traffic .............................................................. 330
show keepalive ............................................................... 586
show keepalive statistics ..................................................... 587
show laep ................................................................. 641
show line ................................................................. 2032
show link-dependency ....................................................... 554
show lldp ................................................................. 569
show lldp dcbx ............................................................... 1185
show lldp interface .......................................................... 569
show lldp local-device ....................................................... 571
show lldp med ............................................................... 572
show lldp med interface ...................................................... 573
show lldp med local-device detail .......................................... 574
show lldp med remote-device ............................................... 575
show lldp remote-device ..................................................... 577
show lldp statistics ........................................................... 579
show lldp tlv-select .......................................................... 1184
show logging ............................................................... 2204
show logging email statistics ............................................... 923
show logging file ............................................................ 2206
show mac address-table ...................................................... 308
show mac address-table address .......................................... 309
show mac address-table count ............................................. 310
show mac address-table dynamic ......................................... 311
show mac address-table interface ......................................... 312
show mac address-table multicast ......................................... 307
show mac address-table static ............................................. 313
show mac address-table vlan ............................................... 314
show mail-server ............................................................ 929
show management access-class ........................................... 1083
show management access-list ............................................. 1084
show memory cpu ........................................................... 2252
show mmrp ................................................................. 1122
show mmrp statistics ........................................................ 1123
show monitor capture ......................................................... 660
show monitor session ......................................................... 662
show msrp ................................................................. 1142
show msrp reservations ....................................................... 1145
show msrp statistics ........................................ 1146
show msrp stream ......................................... 1148
show mvr .................................................... 621
show mvr interface ....................................... 623
show mvr members ........................................ 622
show mvr traffic .......................................... 625
show mvrp .................................................. 1129
show mvrp statistics ..................................... 1130
show nsf .................................................... 2253
show openflow ............................................ 1212
show parser macro ....................................... 1890
show passwords configuration ......................... 1099
show passwords result .................................. 1101
show policy-map .......................................... 737
show policy-map interface ............................... 737
show port protocol ....................................... 816
show port-security ....................................... 315
show power inline ....................................... 2052
show power inline firmware-version .................. 2053
show power-usage-history ............................... 2255
show process app-list .................................... 2256
show process cpu ......................................... 2259
show process proc-list ................................... 2260
show radius statistics .................................... 971
show rmon alarm .......................................... 2061
show rmon alarms ........................................ 2063
show rmon collection history ......................... 2064
show rmon events ........................................ 2065
show rmon hcalarm ....................................... 2066
show rmon history ........................................ 2067
show rmon log ............................................. 2070
show rmon statistics ..................................... 2071
show route-map .......................................... 1548
show router-capability .................................. 1421
show routing heap summary ............................. 1551
show running-config .................................... 1931
show service-acl interface ............................. 287
show service-policy ...................................... 738
show sessions ............................................. 2263
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sflow agent</td>
<td>2134</td>
</tr>
<tr>
<td>show sflow destination</td>
<td>2135</td>
</tr>
<tr>
<td>show sflow polling</td>
<td>2136</td>
</tr>
<tr>
<td>show sflow sampling</td>
<td>2137</td>
</tr>
<tr>
<td>show slot</td>
<td>2264</td>
</tr>
<tr>
<td>show snmp</td>
<td>2141</td>
</tr>
<tr>
<td>show snmp engineid</td>
<td>2142</td>
</tr>
<tr>
<td>show snmp filters</td>
<td>2143</td>
</tr>
<tr>
<td>show snmp group</td>
<td>2144</td>
</tr>
<tr>
<td>show snmp user</td>
<td>2145</td>
</tr>
<tr>
<td>show snmp views</td>
<td>2146</td>
</tr>
<tr>
<td>show sntp configuration</td>
<td>1892</td>
</tr>
<tr>
<td>show sntp server</td>
<td>1893</td>
</tr>
<tr>
<td>show sntp status</td>
<td>1894</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>749</td>
</tr>
<tr>
<td>show spanning-tree summary</td>
<td>757</td>
</tr>
<tr>
<td>show spanning-tree vlan</td>
<td>758</td>
</tr>
<tr>
<td>show startup-config</td>
<td>1933</td>
</tr>
<tr>
<td>show statistics</td>
<td>419</td>
</tr>
<tr>
<td>show statistics port-channel</td>
<td>643</td>
</tr>
<tr>
<td>show statistics switchport</td>
<td>422</td>
</tr>
<tr>
<td>show storm-control</td>
<td>424</td>
</tr>
<tr>
<td>show storm-control action</td>
<td>425</td>
</tr>
<tr>
<td>show support-assist status</td>
<td>2179</td>
</tr>
<tr>
<td>show supported cardtype</td>
<td>2266</td>
</tr>
<tr>
<td>show supported mibs</td>
<td>2119</td>
</tr>
<tr>
<td>show supported switchtype</td>
<td>2268</td>
</tr>
<tr>
<td>show switch</td>
<td>2270</td>
</tr>
<tr>
<td>show switchport protected</td>
<td>431</td>
</tr>
<tr>
<td>show switchport voice</td>
<td>319</td>
</tr>
<tr>
<td>show syslog-servers</td>
<td>2206</td>
</tr>
<tr>
<td>show system</td>
<td>2206</td>
</tr>
<tr>
<td>show system fan</td>
<td>2275</td>
</tr>
<tr>
<td>show system id</td>
<td>2277</td>
</tr>
<tr>
<td>show system internal pktngr</td>
<td>1070</td>
</tr>
<tr>
<td>show system power</td>
<td>2278</td>
</tr>
<tr>
<td>show system temperature</td>
<td>2279</td>
</tr>
<tr>
<td>show tacacs</td>
<td>980</td>
</tr>
<tr>
<td>show tech-support</td>
<td>2281</td>
</tr>
</tbody>
</table>
show time-range .......................................................... 2308
show trapflags ............................................................. 2147
show udld ................................................................. 797
show usb ................................................................. 2312
show users ............................................................... 2284
show users accounts .................................................. 902
show users login-history .............................................. 903
show version ............................................................. 2285
show vlan ................................................................. 818
show vlan association mac ........................................... 820
show vlan association subnet .......................................... 821
show vlan private-vlan ................................................ 822
show vlan remote-span ................................................ 664
show voice vlan ........................................................ 856
show vpc ................................................................. 597
show vpc brief ........................................................... 598
show vpc consistency-features ...................................... 602
show vpc consistency-parameters ................................... 600
show vpc peer-keepalive ............................................... 603
show vpc role ............................................................ 604
show vpc statistics ...................................................... 605
show vrrp ................................................................. 1863
show vrrp interface ..................................................... 1865
show vrrp interface brief .............................................. 1867
show vrrp interface stats ............................................. 1867
shutdown ................................................................. 426
slot ......................................................................... 2239
snmp-server community .............................................. 2149
snmp-server community-group ...................................... 2151
snmp-server contact .................................................... 2152
snmp-server enable traps ............................................ 2153
snmp-server engineID local .......................................... 2156
snmp-server filter ....................................................... 2157
snmp-server group ...................................................... 2159
snmp-server host ....................................................... 2160
snmp-server location .................................................. 2162
snmp-server source-interface ...................................... 2168
snmp-server user ....................................................... 2163
snmp-server v3-host ................................................... 2166
spanning-tree vlan forward-time ........................................... 784
spanning-tree vlan hello-time ............................................. 785
spanning-tree vlan max-age ............................................... 786
spanning-tree vlan priority ............................................... 788
spanning-tree vlan root .................................................... 787
speed .................................................................................. 426, 2033
split-horizon ........................................................................ 1835
stack .................................................................................... 2286
stack-port ............................................................................. 2287
stack-port shutdown ............................................................. 2289
standby .................................................................................. 2290
state ...................................................................................... 2341
storm-control broadcast ......................................................... 1071
storm-control multicast ........................................................ 1072
storm-control unicast ............................................................ 1074
support-assist ....................................................................... 2180
switch renumber ................................................................. 2291
switchport access vlan .......................................................... 823
switchport dot1q ethertype (Global Configuration) ................. 824
switchport dot1q ethertype (Interface Configuration) ............... 826
switchport forbidden vlan ...................................................... 828
switchport general acceptable-frame-type tagged-only ............ 829
switchport general allowed vlan ............................................. 830
switchport general ingress-filtering disable ............................ 831
switchport general pvid ......................................................... 832
switchport mode .................................................................... 833
switchport mode dot1q-tunnel ................................................ 834
switchport mode private-vlan ................................................ 836
switchport port-security (Global Configuration) ..................... 299
switchport port-security (Interface Configuration) .................. 302
switchport private-vlan ......................................................... 837
switchport protected ............................................................. 429
switchport protected name .................................................... 430
switchport trunk ................................................................... 838
switchport trunk encapsulation dot1q ..................................... 838
switchport voice detect auto .................................................. 321
switchport voice vlan ........................................................... 848
switchport voice vlan (Interface) ............................................ 849
switchport voice vlan priority ................................................ 853
system jumbo mtu ................................................. 432
system-mac ......................................................... 607
system-priority ..................................................... 608
T
tacacs-server host .............................................. 981
tacacs-server key ................................................. 982
tacacs-server source-interface ................................. 983
tacacs-server timeout .......................................... 984
telnet ............................................................... 2292
template peer ....................................................... 1421
terminal monitor ................................................ 2207
test copper-port tdr .............................................. 2038
timeout ............................................................. 975, 985
time-range .......................................................... 2304
timers bgp ........................................................... 1423
timers pacing flood .............................................. 1753
timers pacing lsa-group ........................................ 1754
timers spf .......................................................... 1755
timers throttle spf ............................................... 1810
traceroute .......................................................... 2293
traceroute ethernet cfm ...................................... 442
traceroute ipv6 ..................................................... 1606, 2296
traffic-class-group max-bandwidth ......................... 1190
traffic-class-group min-bandwidth ........................... 1192
traffic-class-group strict ....................................... 1193
traffic-class-group weight ..................................... 1195
traffic-shape ....................................................... 739
tunnel destination ............................................... 1838
tunnel mode ipv6ip .............................................. 1839
tunnel source ..................................................... 1839
U
udld enable (Global Config) ................................. 792
udld enable (Interface Config) ................................. 795
udld message time .............................................. 794
udld port ........................................................... 796
udld reset ........................................................... 793
udld timeout interval ......................................... 795
unmount usb ...................................................... 2311
update bootcode ................................................. 2298
url ..................................................................... 1991, 2181
usage ............................................................... 976
user group .......................................................... 1051, 1059
user group moveusers ........................................ 1059
user group name .................................................. 1060
user name ........................................................... 1053
user password .................................................... 1054
user session-timeout ............................................. 1054
user-logout ......................................................... 1052
username .......................................................... 904
username (Mail Server Configuration Mode) ................. 927
username unlock .................................................. 907

V
verification .......................................................... 1044
vlan ................................................................. 840
vlan association mac ............................................. 841
vlan association subnet .......................................... 842
vlan makestatic .................................................... 843
vlan priority ......................................................... 740
vlan protocol group .............................................. 843
vlan protocol group add protocol .............................. 844
vlan protocol group name ...................................... 845
vlan protocol group remove .................................... 846
vpc ................................................................. 609
vpc domain .......................................................... 610
vpc peer-link ....................................................... 611
vrrp accept-mode ................................................. 1853
vrrp authentication .............................................. 1854
vrrp description ................................................... 1855
vrrp ip ................................................................. 1856
vrrp mode ........................................................... 1857
vrrp preempt .......................................................... 1858
vrrp priority .......................................................... 1859
vrrp timers advertise ............................................. 1859
vrrp timers learn .................................................... 1860
vrrp track interface ................................................. 1861
vrrp track ip route ................................................. 1862
W
write .................................................. 1934
write core ......................................... 2125