

Dell PowerConnect 8024/8132/8164 Series Systems CLI Reference Guide

Regulatory Model: PC8024/PC8024F/
PC8132/PC8132F/PC8164/PC8164F
Regulatory Type: XXXXX



Notes



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

Information in this publication is subject to change without notice.

© 2012 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, and PowerConnect™ are trademarks of Dell Inc. StrataXGS® is a registered trademark of Broadcom Corp. sFlow® is a registered trademark of InMon Corporation. Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Regulatory Model PC8024/PC8024F/PC8132/PC8132F/PC8164/PC8164F

Regulatory Type: XXXXX

2012 - June P/N XXXXX Rev. A02

Contents

1	Command Groups	77
	Introduction	77
	Command Groups	77
	Mode Types	81
	Layer 2 Commands	83
	Data Center Technology Commands	117
	Layer 3 Commands	119
	Utility Commands	146
2	Using the CLI	167
	Introduction	167
	Entering and Editing CLI Commands	167
	CLI Command Modes	177
	Starting the CLI	190
	Using CLI Functions and Tools	198

3	Layer 2 Switching Commands	235
4	AAA Commands	237
	TACACS+ Accounting	238
	Commands in this Chapter	239
	aaa authentication dot1x default	240
	aaa authentication enable	241
	aaa authentication login	243
	aaa authorization	245
	aaa authorization network default radius	247
	aaa ias-user username	248
	aaa new-model	249
	clear (IAS)	249
	authorization	250
	enable authentication	251
	enable password	252
	ip http authentication	253
	ip https authentication	254
	login authentication	256
	password (aaa IAS User Configuration)	257
	password (Line Configuration)	258

password (User EXEC)	259
show aaa ias-users	260
show aaa statistics	261
show authentication methods	262
show authorization methods	263
show users accounts	265
show users login-history	266
username	267
username unlock	270
5 Administrative Profiles Commands	271
Overview	271
Commands in this Chapter	272
admin-profile	273
description (Administrative Profile Config)	274
rule	275
show admin-profiles	276
show cli modes	277
6 ACL Commands	279
ACL Logging	279
Commands in this Chapter	282

access-list	282
deny permit (IP ACL)	284
deny permit (Mac-Access-List-Configuration)	286
ip access-group	288
mac access-group	289
mac access-list extended	290
mac access-list extended rename	291
service-acl input	292
show service-acl interface	293
show ip access-lists	294
show mac access-list	295
7 Address Table Commands	297
Commands in this Chapter	298
clear mac address-table	298
mac address-table aging-time	299
mac address-table multicast filtering	300
mac address-table multicast forbidden address	301
mac address-table multicast forbidden	
forward-unregistered	303
mac address-table multicast forward-all	304

mac address-table multicast	
forward-unregistered	305
mac address-table multicast static	306
mac address-table static	307
port security	308
port security max	309
show mac address-table multicast	310
show mac address-table filtering	311
show mac address-table	312
show mac address-table address	313
show mac address-table count	314
show mac address-table dynamic	315
show mac address-table interface	316
show mac address-table static	318
show mac address-table vlan	319
show ports security	320
show ports security addresses	321
8 Auto-VoIP Commands	323
Commands in this Chapter	323
show switchport voice	324
switchport voice detect auto	327

9	CDP Interoperability Commands	329
	Commands in this Chapter	329
	clear isdp counters	329
	clear isdp table	330
	isdp advertise-v2	330
	isdp enable	331
	isdp holdtime	332
	isdp timer	333
	show isdp	333
	show isdp entry	334
	show isdp interface	336
	show isdp neighbors	337
	show isdp traffic	339
10	DHCP Layer 2 Relay Commands	341
	Commands in this Chapter	341
	dhcp l2relay (Global Configuration)	341
	dhcp l2relay (Interface Configuration)	342
	dhcp l2relay circuit-id	343
	dhcp l2relay remote-id	344
	dhcp l2relay trust	344

dhcp l2relay vlan	345
show dhcp l2relay all	346
show dhcp l2relay interface	347
show dhcp l2relay stats interface	348
show dhcp l2relay subscription interface	349
show dhcp l2relay agent-option vlan	350
show dhcp l2relay vlan	351
show dhcp l2relay circuit-id vlan	352
show dhcp l2relay remote-id vlan	353
clear dhcp l2relay statistics interface	354
11 DHCP Management Interface	
Commands	357
Commands in this Chapter	357
release dhcp	358
renew dhcp	359
debug dhcp packet	360
show dhcp lease	361
12 DHCP Snooping Commands	365
Commands in this Chapter	366
clear ip dhcp snooping binding	366

clear ip dhcp snooping statistics	367
ip dhcp snooping	367
ip dhcp snooping binding	368
ip dhcp snooping database	369
ip dhcp snooping database write-delay.	370
ip dhcp snooping limit	371
ip dhcp snooping log-invalid	372
ip dhcp snooping trust	373
ip dhcp snooping verify mac-address	374
show ip dhcp snooping	374
show ip dhcp snooping binding	376
show ip dhcp snooping database	377
show ip dhcp snooping interfaces	377
show ip dhcp snooping statistics	379

13 Dynamic ARP Inspection Commands . . . 383

Commands in this Chapter	383
arp access-list	383
clear ip arp inspection statistics	384
ip arp inspection filter	385
ip arp inspection limit	386
ip arp inspection trust	387

ip arp inspection validate	387
ip arp inspection vlan	388
permit ip host mac host	389
show arp access-list	390
show ip arp inspection	391
show ip arp inspection vlan	394
14 E-mail Alerting Commands	397
Commands in this Chapter	397
logging email	398
logging email urgent	400
logging traps	401
logging email message-type to-addr	402
logging email from-addr	403
logging email message-type subject	403
logging email logtime	404
logging email test message-type	405
show logging email statistics	406
clear logging email statistics	406
security	407
mail-server ip-address hostname	408
port (Mail Server Configuration Mode)	409

username (Mail Server Configuration Mode)	409
password (Mail Server Configuration Mode)	410
show mail-server	411
15 Ethernet Configuration Commands	413
Commands in this Chapter	414
clear counters	414
description	415
duplex	416
flowcontrol	417
interface	418
interface range	419
mtu	420
show interfaces advertise	422
show interfaces configuration	424
show interfaces counters	425
show interfaces description	429
show interfaces detail	430
show interfaces status	433
show statistics	434
show statistics switchport	438
show storm-control	440

shutdown	441
speed	441
storm-control broadcast	443
storm-control multicast	444
storm-control unicast	445
switchport protected	446
switchport protected name	447
show switchport protected	448
16 Ethernet CFM Commands	449
Commands in this Chapter	449
ethernet cfm domain	450
service	451
ethernet cfm cc level	452
ethernet cfm mep level	453
ethernet cfm mep enable	454
ethernet cfm mep active	455
ethernet cfm mep archive-hold-time	456
ethernet cfm mip level	456
ping ethernet cfm	457
traceroute ethernet cfm	458
show ethernet cfm errors	460

show ethernet cfm domain	461
show ethernet cfm maintenance-points local	462
show ethernet cfm maintenance-points remote	463
show ethernet cfm statistics.	464
debug cfm	466
17 Green Ethernet Commands	469
Energy-Detect Mode	469
Energy Efficient Ethernet.	469
Commands in this Chapter.	469
green-mode energy-detect	470
green-mode eee	471
green-mode eee-lpi-history	472
18 GVRP Commands	475
Commands in this Chapter.	475
clear gvrp statistics	475
garp timer	476
gvrp enable (global)	477
gvrp enable (interface).	478
gvrp registration-forbid	479
gvrp vlan-creation-forbid	480

show gvrp configuration	481
show gvrp error-statistics	482
show gvrp statistics	483
19 IGMP Snooping Commands	485
Commands in this Chapter	486
ip igmp snooping (global)	486
ip igmp snooping (interface)	487
ip igmp snooping host-time-out	488
ip igmp snooping leave-time-out	488
ip igmp snooping mrouter-time-out	489
show ip igmp snooping	490
show ip igmp snooping groups	491
show ip igmp snooping interface	492
show ip igmp snooping mrouter	493
ip igmp snooping (VLAN)	494
ip igmp snooping fast-leave	494
ip igmp snooping groupmembership-interval	495
ip igmp snooping maxresponse	496
ip igmp snooping mcartexpiretime	497

20 IGMP Snooping Querier Commands	499
Commands in this Chapter	499
ip igmp snooping querier	499
ip igmp snooping querier election participate	501
ip igmp snooping querier query-interval	502
ip igmp snooping querier timer expiry	503
ip igmp snooping querier version	503
show ip igmp snooping querier	504
21 IP Addressing Commands	507
Commands in this Chapter	507
clear host	508
clear ip address-conflict-detect	508
ip address (Out-of-Band)	509
ip address-conflict-detect run	510
ip address dhcp (Interface Config)	511
ip default-gateway	513
ip domain-lookup	514
ip domain-name	514
ip host	515
ip name-server	516

ipv6 address (Interface Config)	517
ipv6 address (OOB Port)	518
ipv6 address dhcp	520
ipv6 enable (Interface Config)	521
ipv6 enable (OOB Config)	521
ipv6 gateway (OOB Config)	522
show hosts	523
show ip address-conflict	524
show ip helper-address	525
show ipv6 dhcp interface out-of-band statistics	526
show ipv6 interface out-of-band	528
22 IPv6 Access List Commands	529
Commands in this Chapter	529
deny permit (IPv6 ACL)	530
ipv6 access-list	532
ipv6 access-list rename	533
ipv6 traffic-filter	534
show ipv6 access-lists	535
23 IPv6 MLD Snooping Commands	539
Commands in this Chapter	539

ipv6 mld snooping immediate-leave	540
ipv6 mld snooping groupmembership-interval	541
ipv6 mld snooping maxresponse	541
ipv6 mld snooping mcruntime	542
ipv6 mld snooping (Global)	543
ipv6 mld snooping (Interface)	544
ipv6 mld snooping (VLAN)	545
show ipv6 mld snooping	545
show ipv6 mld snooping groups	547
24 IPv6 MLD Snooping Querier	
Commands	549
Commands in this Chapter	549
ipv6 mld snooping querier	550
ipv6 mld snooping querier (VLAN mode)	550
ipv6 mld snooping querier address	551
ipv6 mld snooping querier election participate	552
ipv6 mld snooping querier query-interval	552
ipv6 mld snooping querier timer expiry	553
show ipv6 mld snooping querier	554

25 IP Source Guard Commands	557
Commands in this Chapter.	557
ip verify source	557
ip verify source port-security	558
ip verify binding	559
show ip verify interface	559
show ip verify source interface	560
show ip source binding	561
26 iSCSI Optimization Commands	563
Commands in this Chapter.	564
iscsi aging time	564
iscsi cos	565
iscsi enable	567
iscsi target port	568
show iscsi	570
show iscsi sessions	571
27 Link Dependency Commands	575
Commands in this Chapter.	575
action.	575
link-dependency group	576

add gigabitethernet	577
add tengigabitethernet	577
add port-channel	578
depends-on	579
show link-dependency	580
28 LLDP Commands	583
Commands in this Chapter	584
clear lldp remote-data	584
clear lldp statistics	585
lldp notification	586
lldp notification-interval	586
lldp receive	587
lldp timers	588
lldp transmit	589
lldp transmit-mgmt	590
lldp transmit-tlv	590
show lldp	591
show lldp interface	592
show lldp local-device	593
show lldp remote-device	595
show lldp statistics	597

29 Multicast VLAN Registration	
Commands	601
Commands in this Chapter	602
mvr	602
mvr group	603
mvr mode	604
mvr querytime	604
mvr vlan	606
mvr immediate	606
mvr type	607
mvr vlan group	609
show mvr	610
show mvr members	612
show mvr interface	613
show mvr traffic	615
30 Port Channel Commands	619
Static LAGS	619
VLANs and LAGs	620
LAG Thresholds	620
Port Channels	620
LAG Hashing	621

Enhanced LAG Hashing	622
Manual Aggregation of LAGs	623
Manual Aggregation of LAGs	623
Flexible Assignment of Ports to LAGs	623
Commands in this Chapter	623
channel-group	624
interface port-channel	625
interface range port-channel	625
hashing-mode	626
lacp port-priority	627
lacp system-priority	628
lacp timeout	629
port-channel local-preference	629
port-channel min-links	630
show interfaces port-channel	631
show lacp	633
show statistics port-channel	635
31 Port Monitor Commands	639
Commands in this Chapter	639
monitor session	640
show monitor session	641

32 QoS Commands	643
Access Control Lists	643
Layer 2 ACLs	644
Layer 3/4 IPv4 ACLs	644
Class of Service (CoS)	644
Queue Mapping	645
Commands in this Chapter	646
assign-queue	647
class	647
class-map	648
class-map rename	649
classofservice dot1p-mapping	650
classofservice ip-dscp-mapping	651
classofservice trust	654
conform-color	655
cos-queue min-bandwidth	656
cos-queue random-detect	657
cos-queue strict	658
diffserv	659
drop	660
mark cos	661

mark ip-dscp	661
mark ip-precedence	662
match class-map	663
match cos	664
match destination-address mac	665
match dstip	666
match dstip6	667
match dstl4port	667
match ethertype	668
match ip6flowlbl	669
match ip dscp	670
match ip precedence	671
match ip tos	671
match protocol	672
match source-address mac	673
match srcip	674
match srcip6	675
match srcl4port	675
match vlan	676
mirror	677
police-simple	678

policy-map	679
random-detect queue-parms	680
random-detect exponential-weighting-constant	682
redirect	683
service-policy	684
show class-map	685
show classofservice dot1p-mapping	687
show classofservice ip-dscp-mapping	689
show classofservice trust	692
show diffserv	693
show diffserv service interface	694
show diffserv service interface port-channel	695
show diffserv service brief	696
show interfaces cos-queue	696
show interfaces random-detect	699
show policy-map	700
show policy-map interface	701
show service-policy	702
traffic-shape	703
33 RADIUS Commands	705
Commands in this Chapter	708

aaa accounting dot1x default start-stop	709
accounting	711
acct-port	712
auth-port	713
deadtime	713
debug aaa accounting	714
key	715
msgauth	716
name (RADIUS server)	716
primary	718
priority	718
radius-server attribute 4	719
radius-server deadtime	720
radius-server host	721
radius-server key	722
radius-server retransmit	723
radius-server source-ip	724
radius-server timeout	724
retransmit	725
show aaa servers	726
show accounting methods	728

show radius statistics	729
source-ip	733
timeout	734
usage	735
34 Spanning Tree Commands	737
Commands in this Chapter	738
clear spanning-tree detected-protocols	739
exit (mst)	740
instance (mst)	740
name (mst)	742
revision (mst)	743
show spanning-tree	744
show spanning-tree summary	751
spanning-tree	752
spanning-tree auto-portfast	753
spanning-tree bpdu flooding	754
spanning-tree bpdu-protection	754
spanning-tree cost	755
spanning-tree disable	756
spanning-tree forward-time	757
spanning-tree guard	758

spanning-tree loopguard	759
spanning-tree max-age	760
spanning-tree max-hops	760
spanning-tree mode	761
spanning-tree mst configuration	762
spanning-tree mst cost	763
spanning-tree mst port-priority	764
spanning-tree mst priority	765
spanning-tree portfast	766
spanning-tree portfast bpdudfilter default	767
spanning-tree portfast default	767
spanning-tree port-priority	768
spanning-tree priority	769
spanning-tree tcnguard	770
spanning-tree transmit hold-count	771
35 TACACS+ Commands	773
Commands in this Chapter	773
key	774
port	774
priority	775
show tacacs	776

tacacs-server host	777
tacacs-server key	778
tacacs-server timeout	779
timeout	779
36 UDLD Commands	781
Detecting Unidirectional Links on a Device Port	781
Processing UDLD Traffic from Neighbors	782
UDLD in Normal-mode	782
UDLD in Aggressive-mode	782
Commands in this Chapter	783
udld enable (Global Config)	783
udld reset	784
udld message time	785
udld timeout interval	785
udld enable (Interface Config)	786
udld port	787
show udld	788
debug udld	789
37 VLAN Commands	791
Double VLAN Mode	791

Independent VLAN Learning	792
Protocol Based VLANs.	792
IP Subnet Based VLANs	793
MAC-Based VLANs	793
Private VLAN Commands	793
Commands in this Chapter.	796
dvlan-tunnel ethertype.	797
interface vlan.	798
interface range vlan	799
mode dvlan-tunnel	800
name (VLAN Configuration)	801
protocol group	802
protocol vlan group	803
protocol vlan group all.	804
show dvlan-tunnel	805
show dvlan-tunnel interface.	806
show interfaces switchport	807
show port protocol.	811
show vlan	812
show vlan association mac	814
show vlan association subnet	815

switchport access vlan	816
switchport forbidden vlan	817
switchport general acceptable-frame-type	
tagged-only	818
switchport general allowed vlan	818
switchport general ingress-filtering disable	819
switchport general pvid	820
switchport mode	821
switchport trunk	822
vlan	824
vlan (Global Config)	825
vlan association mac	826
vlan association subnet	826
vlan database	827
vlan makestatic	828
vlan protocol group	829
vlan protocol group add protocol	830
vlan protocol group name	831
vlan protocol group remove	831
switchport private-vlan	832
switchport mode private-vlan	833

private-vlan	834
show vlan private-vlan	836
38 Voice VLAN Commands	839
Commands in this Chapter	840
voice vlan	840
voice vlan (Interface)	840
voice vlan data priority	842
show voice vlan	842
39 802.1x Commands	845
Local 802.1X Authentication Server	845
MAC Authentication Bypass	846
Guest VLAN	847
802.1x Monitor Mode	847
RADIUS-based Dynamic VLAN Assignment	848
Commands in this Chapter	848
dot1x dynamic-vlan enable	849
dot1x initialize	850
dot1x mac-auth-bypass	850
dot1x max-req	851
dot1x max-users	852

dot1x port-control	853
dot1x re-authenticate	854
dot1x reauthentication.	855
dot1x system-auth-control.	855
dot1x system-auth-control monitor	856
dot1x timeout guest-vlan-period	857
dot1x timeout quiet-period	858
dot1x timeout re-authperiod.	859
dot1x timeout server-timeout	860
dot1x timeout supp-timeout	860
dot1x timeout tx-period	861
show dot1x.	862
show dot1x authentication-history	864
show dot1x clients.	866
show dot1x interface	869
show dot1x interface statistics	871
show dot1x users	873
clear dot1x authentication-history	874
dot1x guest-vlan	875
dot1x unauth-vlan	876
show dot1x advanced	877

40	Data Center Technology Commands . . .	879
41	Data Center Bridging Commands	881
	Data Center Bridging Exchange Protocol	881
	Interoperability with IEEE DCBX	885
	Port Roles	885
	Commands in this Chapter	889
	Data Center Bridging Capability Exchange Commands	889
	datacenter-bridging	889
	lldp dcbx version	890
	lldp tlv-select dcbxp	891
	lldp dcbx port-role	893
	show lldp tlv-select	894
	show lldp dcbx	895
	Enhanced Transmission Selection Commands	901
	classofservice traffic-class-group	901
	traffic-class-group max-bandwidth	902
	traffic-class-group min-bandwidth	904
	traffic-class-group strict	905
	traffic-class-group weight	907
	show classofservice traffic-class-group	908

show interfaces traffic-class-group	909
42 FIP Snooping Commands	913
Setting Up FIP Snooping	913
Commands in this Chapter	914
feature fip-snooping	915
fip-snooping enable	916
fip-snooping fc-map	917
fip-snooping port-mode	918
show fip-snooping	919
show fip-snooping enode	921
show fip-snooping fcf	923
show fip-snooping sessions	926
show fip-snooping statistics	934
show fip-snooping vlan	941
clear fip-snooping statistics	943
43 Priority Flow Control Commands	945
Commands in this Chapter	946
priority-flow-control mode	946
priority-flow-control priority	947
clear priority-flow-control statistics	949

show interfaces priority-flow-control	949
44 Layer 3 Commands	953
45 ARP Commands	955
ARP Aging	956
Commands in this Chapter	956
arp	956
arp cachesize	957
arp dynamicrenew	958
arp purge	959
arp resptime	960
arp retries	961
arp timeout	961
clear arp-cache	962
clear arp-cache management	963
ip local-proxy-arp	964
ip proxy-arp	964
show arp	965

46 DHCP Server and Relay Agent	
Commands	967
Commands in this Chapter	968
ip dhcp pool	968
bootfile	971
clear ip dhcp binding	972
clear ip dhcp conflict	973
client-identifier	973
client-name	974
default-router	975
dns-server (IP DHCP Pool Config)	976
domain-name (IP DHCP Pool Config)	977
hardware-address	977
host	978
ip dhcp bootp automatic	979
ip dhcp conflict logging	980
ip dhcp excluded-address	981
ip dhcp ping packets	982
lease	983
netbios-name-server	984
netbios-node-type	985
network	986

next-server	986
option	987
service dhcp	991
sntp	992
show ip dhcp binding	993
show ip dhcp conflict	994
show ip dhcp global configuration	994
show ip dhcp pool	995
show ip dhcp server statistics	996
47 DHCPv6 Commands	999
clear ipv6 dhcp	999
dns-server (IPv6 DHCP Pool Config)	1000
domain-name (IPv6 DHCP Pool Config)	1000
ipv6 dhcp pool	1001
ipv6 dhcp relay	1002
ipv6 dhcp server	1003
prefix-delegation	1004
service dhcpv6	1006
show ipv6 dhcp	1007
show ipv6 dhcp binding	1007
show ipv6 dhcp interface (User EXEC)	1008

show ipv6 dhcp interface (Privileged EXEC)	1010
show ipv6 dhcp pool	1016
show ipv6 dhcp statistics	1016
48 DVMRP Commands	1019
Commands in this Chapter	1019
ip dvmrp	1019
ip dvmrp metric	1020
show ip dvmrp	1021
show ip dvmrp interface	1022
show ip dvmrp neighbor	1022
show ip dvmrp nexthop	1023
show ip dvmrp prune	1024
show ip dvmrp route	1025
49 IGMP Commands	1027
Commands in this Chapter	1028
ip igmp	1028
ip igmp last-member-query-count	1029
ip igmp last-member-query-interval	1030
ip igmp query-interval	1031
ip igmp query-max-response-time	1032

ip igmp robustness	1032
ip igmp startup-query-count	1033
ip igmp startup-query-interval	1034
ip igmp version	1035
show ip igmp	1035
show ip igmp groups	1036
show ip igmp interface	1038
show ip igmp membership	1039
show ip igmp interface stats	1040
50 IGMP Proxy Commands	1043
Commands in this Chapter	1043
ip igmp-proxy	1043
ip igmp-proxy reset-status	1044
ip igmp-proxy unsolicited-report-interval	1045
show ip igmp-proxy	1046
show ip igmp-proxy interface	1047
show ip igmp-proxy groups	1048
show ip igmp-proxy groups detail	1049
51 IP Helper/DHCP Relay Commands	1051
Commands in this Chapter	1053

bootpdhcprelay maxhopcount	1053
bootpdhcprelay minwaittime	1054
clear ip helper statistics	1055
ip dhcp relay information check	1055
ip dhcp relay information check-reply	1056
ip dhcp relay information option	1057
ip dhcp relay information option-insert	1058
ip helper-address (global configuration)	1059
ip helper-address (interface configuration)	1061
ip helper enable	1063
show ip helper-address	1064
show ip dhcp relay	1065
show ip helper statistics	1066
52 IP Routing Commands	1069
Static Routes/ECMP Static Routes	1069
Static Reject Routes	1070
Default Routes	1070
Commands in this Chapter	1070
encapsulation	1070
ip address	1071
ip mtu	1072

ip netdirbcast	1074
ip route	1074
ip route default	1076
ip route distance	1077
ip routing	1078
show ip brief	1078
show ip interface	1079
show ip protocols	1082
show ip route	1087
show ip route configured	1089
show ip route connected	1090
show ip route preferences	1091
show ip route summary	1092
show ip traffic	1093
show ip vlan	1095
53 IPv6 Routing Commands	1097
IPv6 Limitations & Restrictions	1097
Commands in this Chapter	1097
clear ipv6 neighbors	1098
clear ipv6 statistics	1099
ipv6 address	1100

ipv6 enable	1101
ipv6 hop-limit	1102
ipv6 host	1102
ipv6 mld last-member-query-count	1103
ipv6 mld last-member-query-interval	1104
ipv6 mld-proxy	1105
ipv6 mld-proxy reset-status	1105
ipv6 mld-proxy unsolicit-rprt-interval.	1106
ipv6 mld query-interval	1107
ipv6 mld query-max-response-time	1107
ipv6 mld router	1108
ipv6 mtu	1109
ipv6 nd dad attempts.	1110
ipv6 nd managed-config-flag	1111
ipv6 nd ns-interval	1111
ipv6 nd other-config-flag	1112
ipv6 nd prefix.	1113
ipv6 nd ra-interval	1114
ipv6 nd ra-lifetime	1115
ipv6 nd reachable-time	1116
ipv6 nd suppress-ra	1117

ipv6 route	1118
ipv6 route distance	1119
ipv6 unicast-routing	1120
ping ipv6	1121
ping ipv6 interface	1122
show ipv6 brief	1123
show ipv6 interface	1124
show ipv6 interface management statistics	1127
show ipv6 mld groups	1128
show ipv6 mld interface	1131
show ipv6 mld-proxy	1134
show ipv6 mld-proxy groups	1135
show ipv6 mld-proxy groups detail	1137
show ipv6 mld-proxy interface	1139
show ipv6 mld traffic	1140
show ipv6 neighbors	1141
show ipv6 route	1142
show ipv6 route preferences	1144
show ipv6 route summary	1145
show ipv6 traffic	1146
show ipv6 vlan	1149

traceroute ipv6	1149
54 Loopback Interface Commands	1151
Commands in this Chapter	1151
interface loopback	1151
show interfaces loopback	1152
55 Multicast Commands	1155
Commands in this Chapter	1156
ip mcast boundary	1157
ip mroute	1157
ip multicast	1158
ip multicast ttl-threshold	1159
ip pim	1160
ip pim bsr-border	1161
ip pim bsr-candidate	1161
ip pim dense	1163
ip pim dr-priority	1163
ip pim hello-interval	1164
ip pim join-prune-interval	1165
ip pim register-rate-limit	1166
ip pim rp-address	1166

ip pim rp-candidate	1167
ip pim sparse	1168
ip pim ssm	1169
ip pim spt-threshold	1170
show ip multicast	1171
show ip mcast boundary	1172
show ip multicast interface	1172
show ip mcast mroute	1173
show ip mcast mroute group	1174
show ip mcast mroute source	1175
show ip mcast mroute static	1176
show ip pim bsr-router	1177
show ip pim interface	1178
show ip pim neighbor	1180
show ip pim rp hash	1181
show ip pim rp mapping	1182
56 IPv6 Multicast Commands	1185
ipv6 pim (Global config)	1185
ipv6 pim (VLAN Interface config)	1186
ipv6 pim bsr-border	1187
ipv6 pim bsr-candidate	1187

ipv6 pim dense	1188
ipv6 pim dr-priority	1189
ipv6 pim hello-interval	1190
ipv6 pim join-prune-interval	1190
ipv6 pim register-rate-limit	1191
ipv6 pim register-threshold	1192
ipv6 pim rp-address	1193
ipv6 pim rp-candidate	1193
ipv6 pim sparse (Global config)	1194
ipv6 pim spt-threshold	1195
ipv6 pim ssm	1196
show ipv6 pim	1196
show ipv6 pim bsr	1198
show ipv6 pim bsr-router	1198
show ipv6 pim interface	1200
show ipv6 pim neighbor	1201
show ipv6 pim rphash	1202
show ipv6 pim rp mapping	1202
57 OSPF Commands	1205
Route Preferences	1206
OSPF Equal Cost Multipath (ECMP)	1206

Forwarding of OSPF Opaque LSAs Enabled by	
Default	1207
Passive Interfaces	1207
Graceful Restart	1208
Commands in this Chapter	1208
area default-cost (Router OSPF)	1209
area nssa (Router OSPF)	1210
area nssa default-info-originate (Router OSPF Config)	1212
area nssa no-redistribute	1213
area nssa no-summary	1214
area nssa translator-role	1214
area nssa translator-stab-intv	1215
area range (Router OSPF)	1216
area stub	1220
area stub no-summary	1221
area virtual-link	1221
area virtual-link authentication	1224
area virtual-link dead-interval	1225
area virtual-link hello-interval	1226
area virtual-link retransmit-interval	1227

area virtual-link transmit-delay	1228
auto-cost	1229
bandwidth	1230
capability opaque	1230
clear ip ospf	1231
clear ip ospf stub-router	1232
compatible rfc1583.	1233
default-information originate (Router OSPF Configuration)	1234
default-metric	1235
distance ospf.	1236
distribute-list out	1237
enable	1238
exit-overflow-interval	1239
external-lsdb-limit.	1239
ip ospf area.	1240
ip ospf authentication	1241
ip ospf cost.	1242
ip ospf database-filter all out	1243
ip ospf dead-interval.	1243
ip ospf hello-interval.	1244

ip ospf mtu-ignore	1245
ip ospf network	1246
ip ospf priority	1247
ip ospf retransmit-interval	1247
ip ospf transmit-delay	1248
log adjacency-changes	1249
max-metric router-lsa	1250
maximum-paths	1252
network area	1253
nsf	1254
nsf helper	1255
nsf helper strict-lsa-checking	1256
nsf restart-interval	1256
passive-interface default	1257
passive-interface	1258
redistribute	1259
router-id	1260
router ospf	1261
show ip ospf	1261
show ip ospf abr	1269
show ip ospf area	1270

show ip ospf asbr	1273
show ip ospf database	1274
show ip ospf database database-summary	1277
show ip ospf interface	1279
show ip ospf interface brief	1281
show ip ospf interface stats	1283
show ip ospf neighbor	1284
show ip ospf range	1287
show ip ospf statistics	1289
show ip ospf stub table	1291
show ip ospf traffic	1292
show ip ospf virtual-link	1294
show ip ospf virtual-links brief	1296
show routing heap summary	1297
timers pacing flood	1298
timers pacing lsa-group	1299
timers spf	1300
58 OSPFv3 Commands	1301
area default-cost (Router OSPFv3)	1302
area nssa (Router OSPFv3)	1303

area nssa default-info-originate (Router OSPFv3 Config)	1304
area nssa no-redistribute	1305
area nssa no-summary	1306
area nssa translator-role	1307
area nssa translator-stab-intv	1308
area range (Router OSPFv3)	1309
area stub	1310
area stub no-summary	1311
area virtual-link	1312
area virtual-link dead-interval	1314
area virtual-link hello-interval	1314
area virtual-link retransmit-interval	1315
area virtual-link transmit-delay	1316
default-information originate (Router OSPFv3 Configuration)	1317
default-metric	1318
distance ospf	1319
enable	1320
exit-overflow-interval	1321
external-lsdb-limit	1322

ipv6 ospf	1322
ipv6 ospf area	1323
ipv6 ospf cost	1324
ipv6 ospf dead-interval	1325
ipv6 ospf hello-interval	1326
ipv6 ospf mtu-ignore	1326
ipv6 ospf network	1327
ipv6 ospf priority	1328
ipv6 ospf retransmit-interval	1329
ipv6 ospf transmit-delay	1330
ipv6 router ospf	1331
maximum-paths	1331
nsf	1332
nsf helper	1333
nsf helper strict-lsa-checking	1334
nsf restart-interval	1335
passive-interface	1335
passive-interface default	1336
redistribute	1337
router-id	1338
show ipv6 ospf	1338

show ipv6 ospf abr	1343
show ipv6 ospf area	1344
show ipv6 ospf asbr	1345
show ipv6 ospf border-routers	1346
show ipv6 ospf database	1346
show ipv6 ospf database database-summary	1351
show ipv6 ospf interface	1352
show ipv6 ospf interface brief	1353
show ipv6 ospf interface stats	1354
show ipv6 ospf interface vlan	1356
show ipv6 ospf neighbor	1357
show ipv6 ospf range	1359
show ipv6 ospf stub table	1360
show ipv6 ospf virtual-links	1361
show ipv6 ospf virtual-link brief	1362

59 Router Discovery Protocol 1365

Commands 1365

Commands in this Chapter	1365
ip irdp	1365
ip irdp address	1367
ip irdp holdtime	1368

ip irdp maxadvertinterval	1369
ip irdp minadvertinterval	1370
ip irdp multicast	1371
ip irdp preference	1372
show ip irdp	1372
60 Routing Information Protocol	
Commands	1375
Commands in this Chapter	1375
auto-summary	1375
default-information originate (Router RIP	
Configuration)	1376
default-metric	1377
distance rip	1378
distribute-list out	1378
enable	1379
hostroutesaccept	1380
ip rip	1381
ip rip authentication	1381
ip rip receive version	1382
ip rip send version	1383
redistribute	1384

router rip	1385
show ip rip	1386
show ip rip interface	1387
show ip rip interface brief	1388
split-horizon	1389
61 Tunnel Interface Commands	1391
Commands in this Chapter	1391
interface tunnel	1392
show interfaces tunnel	1392
tunnel destination	1393
tunnel mode ipv6ip	1394
tunnel source	1395
62 Virtual Router Redundancy Protocol Commands	1397
Pingable VRRP Interface	1397
VRRP Route/Interface Tracking	1398
Interface Tracking	1399
Route Tracking	1399
Commands in this Chapter	1399
ip vrrp	1400

vrrp accept-mode	1400
vrrp authentication	1401
vrrp description	1402
vrrp ip	1403
vrrp mode	1405
vrrp preempt	1405
vrrp priority	1406
vrrp timers advertise	1407
vrrp timers learn	1408
vrrp track interface	1409
vrrp track ip route	1410
show vrrp	1412
show vrrp interface	1415
show vrrp interface brief	1417
show vrrp interface stats	1418
ip vrrp accept-mode	1419
show ip vrrp interface	1420
63 Utility Commands	1423
64 Auto-Install Commands	1425
Commands in this Chapter	1426

boot auto-copy-sw	1426
boot auto-copy-sw allow-downgrade	1427
boot host autoreboot	1428
boot host autosave	1429
boot host dhcp	1429
boot host retrycount	1430
show auto-copy-sw	1431
show boot	1432

65 Captive Portal Commands 1435

Commands in this Chapter	1435
authentication timeout	1437
captive-portal	1437
enable	1438
http port	1439
https port	1439
show captive-portal	1440
show captive-portal status	1441
block	1442
configuration	1443
enable	1443
group	1444

interface	1445
locale	1445
name (Captive Portal)	1446
protocol	1447
redirect	1447
redirect-url	1448
session-timeout	1448
verification	1449
captive-portal client deauthenticate	1450
show captive-portal client status	1450
show captive-portal configuration client status	1451
show captive-portal interface client status	1452
show captive-portal interface configuration	
status	1454
clear captive-portal users	1455
no user	1455
show captive-portal user	1456
user group	1457
user-logout	1458
user name	1459
user password	1460

user session-timeout	1460
show captive-portal configuration	1461
show captive-portal configuration interface	1462
show captive-portal configuration locales	1463
show captive-portal configuration status	1464
user group	1466
user group moveusers	1466
user group name	1467
66 CLI Macro Commands	1469
Commands in this Chapter	1470
macro name	1470
macro global apply	1471
macro global trace	1472
macro global description	1473
macro apply	1474
macro trace	1475
macro description	1476
show parser macro	1476
67 Clock Commands	1479
Real-time Clock	1479

Simple Network Time Protocol	1479
Commands in this Chapter.	1480
show sntp configuration.	1480
show sntp server.	1481
show sntp status.	1483
sntp authenticate	1484
sntp authentication-key	1485
sntp broadcast client enable	1486
sntp client poll timer.	1487
sntp server	1487
sntp trusted-key	1488
sntp unicast client enable.	1489
clock timezone hours-offset.	1490
no clock timezone	1490
clock summer-time recurring	1491
clock summer-time date.	1492
no clock summer-time.	1493
show clock.	1494
68 Command Line Configuration Scripting	
Commands	1497
Commands in this Chapter.	1497

script apply	1497
script delete	1498
script list	1499
script show	1499
script validate	1500
69 Configuration and Image File Commands	1503
File System Commands	1503
Command Line Interface Scripting	1503
Commands in this Chapter	1503
boot system	1504
clear config	1505
copy	1506
delete	1513
delete backup-config	1514
delete backup-image	1514
delete startup-config	1515
dir	1515
erase	1516
filedescr	1517
rename	1518

show backup-config	1519
show bootvar	1520
show running-config	1521
show startup-config	1522
update bootcode	1524
write	1525
70 Denial of Service Commands	1527
Commands in this Chapter	1528
dos-control firstfrag	1529
dos-control icmp	1529
dos-control l4port	1530
dos-control sipdip	1531
dos-control tcpflag	1532
dos-control tcpfrag	1532
ip icmp echo-reply	1533
ip icmp error-interval	1534
ip unreachable	1535
ip redirects	1535
ipv6 icmp error-interval	1536
ipv6 unreachable	1537
show dos-control	1537

71 Line Commands	1539
exec-timeout	1539
history	1540
history size	1541
line	1541
show line	1542
speed	1544
72 Management ACL Commands	1545
Commands in this Chapter	1545
deny (management)	1546
management access-class	1547
management access-list	1548
permit (management)	1549
show management access-class	1551
show management access-list	1552
73 Mode Commands	1555
configure terminal	1555
do	1555

74 Password Management Commands . . .	1559
Configurable Minimum Password Length	1559
Password History	1559
Password Aging	1559
User Lockout	1559
Password Strength	1560
Commands in this Chapter	1561
passwords aging	1562
passwords history	1562
passwords lock-out	1563
passwords min-length	1564
passwords strength-check	1565
passwords strength minimum uppercase-letters . . .	1566
passwords strength minimum lowercase-letters . . .	1567
passwords strength minimum	
numeric-characters	1568
passwords strength minimum special-characters . . .	1569
passwords strength max-limit	
consecutive-characters	1569
passwords strength max-limit	
repeated-characters	1570

passwords strength minimum	
character-classes	1571
passwords strength exclude-keyword	1572
enable password encrypted	1573
show passwords configuration	1574
show passwords result	1576
75 PHY Diagnostics Commands	1579
show copper-ports tdr	1579
show fiber-ports optical-transceiver	1580
test copper-port tdr.	1581
76 RMON Commands	1583
Commands in this Chapter	1583
rmon alarm	1583
rmon collection history	1586
rmon event	1587
show rmon alarm.	1588
show rmon alarms	1590
show rmon collection history	1591
show rmon events	1592
show rmon history	1594

show rmon log	1597
show rmon statistics.	1598
77 SDM Templates Commands	1603
Commands in this Chapter.	1603
sdm prefer	1603
show sdm prefer	1605
78 Serviceability Tracing Packet Commands	1609
Commands in this Chapter.	1609
debug arp	1610
debug auto-voip	1611
debug clear	1611
debug console	1612
debug dot1x	1612
debug igmpsnooping.	1613
debug ip acl	1614
debug ip dvmrp.	1614
debug ip igmp	1615
debug ip mcache.	1616
debug ip pimdm packet	1617

debug ip pimsm packet	1618
debug ip vrrp	1618
debug ipv6 dhcp	1619
debug ipv6 mcache	1620
debug ipv6 mld	1620
debug ipv6 pimdm	1621
debug ipv6 pimsm	1622
debug isdp	1623
debug lacp	1624
debug mldsnooping	1624
debug ospf	1625
debug ospfv3	1626
debug ping	1626
debug rip	1627
debug sflow	1628
debug spanning-tree	1628
debug vrrp	1629
show debugging	1629
79 Sflow Commands	1631
Commands in this Chapter	1631
sflow destination	1631

sflow polling	1633
sflow polling (Interface Mode)	1634
sflow sampling	1635
sflow sampling (Interface Mode)	1636
show sflow agent	1637
show sflow destination	1638
show sflow polling	1639
show sflow sampling	1640
80 SNMP Commands	1643
Commands in this Chapter	1643
show snmp	1643
show snmp engineID	1645
show snmp filters	1646
show snmp group	1647
show snmp user	1649
show snmp views	1651
show trapflags	1652
snmp-server community	1654
snmp-server community-group	1656
snmp-server contact	1657
snmp-server enable traps	1657

snmp-server engineID local	1660
snmp-server filter	1661
snmp-server group	1663
snmp-server host	1664
snmp-server location	1666
snmp-server user	1667
snmp-server view	1668
snmp-server v3-host	1670
81 SSH Commands	1673
Commands in this Chapter	1673
crypto key generate dsa	1673
crypto key generate rsa	1674
crypto key pubkey-chain ssh	1675
ip ssh port	1676
ip ssh pubkey-auth	1677
ip ssh server	1677
key-string	1678
show crypto key mypubkey	1680
show crypto key pubkey-chain ssh	1681
show ip ssh	1682
user-key	1683

82 Syslog Commands	1685
CLI Logged to Local File and Syslog Server	1685
Commands in this Chapter	1686
clear logging	1687
clear logging file	1687
description (Logging)	1688
level	1689
logging cli-command	1689
logging	1692
logging audit	1694
logging buffered	1694
logging console	1696
logging facility	1697
logging file	1698
logging monitor	1699
logging on	1700
logging snmp	1701
logging web-session	1701
port	1702
show logging	1703
show logging file	1704

show syslog-servers	1705
terminal monitor	1706
83 System Management Commands	1707
asset-tag	1707
banner exec	1708
banner login	1709
banner motd	1710
banner motd acknowledge	1711
clear checkpoint statistics	1714
cut-through mode	1715
exec-banner	1715
hardware profile portmode	1716
hostname	1717
initiate failover	1718
locate	1719
login-banner	1719
media-type	1720
member	1721
motd-banner	1722
nsf	1723
ping	1724

reload	1725
set description	1726
slot	1727
show banner	1728
show boot-version	1730
show checkpoint statistics	1730
show cut-through mode	1731
show hardware profile	1732
show interfaces advanced firmware	1733
show interfaces media-type	1734
show memory cpu	1735
show nsf	1736
show power-usage-history	1737
show process cpu	1738
show sessions	1742
show slot	1743
show supported cardtype	1744
show supported switchtype	1745
show switch	1747
show system	1757
show system fan	1757

show system id	1758
show system power	1759
show system temperature	1760
show tech-support	1762
show users	1765
show version	1766
stack	1767
stack-port	1768
standby	1769
switch renumber	1770
telnet	1770
traceroute	1773
84 Telnet Server Commands	1777
Telnet Client Behaviors	1777
Commands in this Chapter	1780
ip telnet server disable	1780
ip telnet port	1781
show ip telnet	1781
85 Terminal Length Commands	1783
terminal length	1783

86	Time Ranges Commands	1785
	time-range	1785
	absolute	1786
	periodic	1787
	show time-range	1789
87	User Interface Commands	1793
	enable	1793
	end	1794
	exit	1794
	quit	1795
88	Web Server Commands	1797
	Web Sessions	1797
	Commands in this Chapter	1798
	common-name	1798
	country	1799
	crypto certificate generate	1800
	crypto certificate import	1801
	crypto certificate request	1803
	duration	1804
	ip http port	1804

ip http server	1805
ip http secure-certificate	1806
ip http secure-port	1807
ip http secure-server	1808
key-generate	1808
location	1809
organization-unit	1810
show crypto certificate mycertificate	1811
show ip http server status	1812
show ip http server secure status	1812
state	1814

A Appendix A: List of Commands	1817
---	-------------

Command Groups

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 similar to the UNIX C shell.

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 EIA/TIA-232 port or through a Telnet/SSH session.

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

This guide also provides information for configuring the PowerConnect switch, details the procedures, and provides configuration examples. Basic installation configuration is described in the *User's Guide* and must be completed before using this document.

Command Groups

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

Table 1-1. System Command Groups

Command Group	Description
Layer 2 Commands	
AAA	Configures connection security including authorization and passwords.
Administrative Profiles Commands	Group commands into a profile and assign a profile to a user upon authentication.

Table 1-1. System Command Groups (continued)

Command Group	Description
Administrative Profiles	Configures and displays ACL information.
Address Table	Configures bridging address tables.
Auto-VoIP	Configures Auto VoIP for IP phones on a switch.
CDP Interoperability	Configures Cisco® Discovery Protocol (CDP).
DHCP L2 Relay	Enables the Layer 2 DHCP Relay agent for an interface.
DHCP Management Interface	Configures DHCP snooping and whether an interface is trusted for filtering.
Dynamic ARP Inspection	Configures for rejection of invalid and malicious ARP packets.
Ethernet Configuration	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.
Ethernet CFM	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IGMP Snooping Querier	Configures IGMP Snooping Querier and displays IGMP Snooping Querier information.
IP Addressing	Configures and manages IP addresses on the switch.
IPv6 ACL	Configures and displays ACL information for IPv6.
IPv6 MLD Snooping	Configures IPv6 MLD Snooping.
IPv6 MLD Snooping Querier	Configures IPv6 Snooping Querier and displays IPv6 Snooping Querier information.
iSCSI Optimization	Configures special QoS treatment for traffic between iSCSI initiators and target systems.
Link Dependency	Configures and displays link dependency information.
LLDP	Configures and displays LLDP information.
Port Channel	Configures and displays Port channel information.
Port Monitor	Monitors activity on specific target ports.
QoS	Configures and displays QoS information.

Table 1-1. System Command Groups (continued)

Command Group	Description
RADIUS	Configures and displays RADIUS information.
Spanning Tree	Configures and reports on Spanning Tree protocol.
TACACS+	Configures and displays TACACS+ information.
VLAN	Configures VLANs and displays VLAN information.
802.1x	Configures and displays commands related to 802.1x security protocol.
Data Center Technology Commands	
Data Center Bridging Commands	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.
FIP Snooping Commands	FCoE Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance. FIP snooping is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following recommendations in Annex C of FC_BB_5 Rev 2.00
Priority Flow Control Commands	Provides priority-based flow control that can pause (inhibit transmission of) individual priorities within a single physical link.
Layer 3 Commands	
ARP (IPv4)	Manages Address Resolution Protocol functions.
DHCP Server and Relay Agent (IPv4)	Manages DHCP/BOOTP operations on the system.
DHCPv6	Configures IPv6 DHCP functions.
DVMRP (Mcast)	Configures DVMRP operations.
IGMP (Mcast)	Configures IGMP operations.
IGMP Proxy (Mcast)	Manages IGMP Proxy on the system.
IP Helper/DHCP Relay	Configures relay of UDP packets.

Table 1-1. System Command Groups (continued)

Command Group	Description
IP Routing (IPv4)	Configures IP routing and addressing.
IPv6 Multicast	Manages IPv6 Multicasting on the system.
IPv6 Routing	Configures IPv6 routing and addressing.
Loopback Interface (IPv6)	Manages Loopback configurations.
Multicast (Mcast)	Manages Multicasting on the system.
OSPF (IPv4)	Manages shortest path operations.
OSPFv3 (IPv6)	Manages IPv6 shortest path operations.
Router Discovery Protocol (IPv4)	Manages router discovery operations.
Routing Information Protocol (IPv4)	Configures RIP activities.
Tunnel Interface (IPv6)	Managing tunneling operations.
Virtual Router Redundancy (IPv4)	Controls virtual LAN routing.
Virtual Router Redundancy (IPv4)	Manages router redundancy on the system.
Utility Commands	
Auto-Install	Automatically configures switch when a configuration file is not found.
Captive Portal	Blocks clients from accessing network until user verification is established.
Clock	Configures the system clock.
Command Line Configuration Scripting	Manages the switch configuration files.
Denial of Service	Provides several Denial of Service options.
Line	Configures the console, SSH, and remote Telnet connection.
Management ACL	Configures and displays management access-list information.

Table 1-1. System Command Groups (continued)

Command Group	Description
Password Management	Provides password management.
PHY Diagnostics	Diagnoses and displays the interface status.
RMON	Can be configured through the CLI and displays RMON information.
Serviceability Tracing	Controls display of debug output to serial port or telnet console.
sFlow	Configures sFlow monitoring.
SNMP	Configures SNMP communities, traps and displays SNMP information.
SSH	Configures SSH authentication.
Syslog	Manages and displays syslog messages.
System Management	Configures the switch clock, name and authorized users.
Telnet Server	Configures Telnet service on the switch and displays Telnet information.
User Interface	Describes user commands used for entering CLI commands.
Web Server	Configures web-based access to the switch.

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
- CC — Crypto Configuration
- CP — Captive Portal Configuration
- CPI — Captive Portal Instance
- CMC — Class-Map Configuration
- DP — IP DHCP Pool Configuration

- GC — Global Configuration
- IC — Interface Configuration (reached via **interface vlan xxx** command)
- IP — IP Access List Configuration
- IR — Interface Range
- KC — Key Chain
- KE — Key
- L — Logging
- LC — Line Configuration
- LD — Link Dependency
- MA — Management Access-level
- MC — MST Configuration
- MDC — Maintenance Domain Configuration
- ML — MAC-List Configuration
- MSC — Mail Server Configuration
- MT — MAC-acl
- OG — OSPFv2 Global Configuration
- PE — Privileged EXEC
- PM — Policy Map Configuration
- PCGC — Policy Map Global Configuration
- PCMC — Policy Class Map Configuration
- R — Radius
- RIP — Router RIP Configuration
- RC — Router Configuration
- ROSPF — Router Open Shortest Path First
- ROSV3 — Router Open Shortest Path First Version 3
- SG — Stack Global Configuration
- SP — SSH Public Key
- SK — SSH Public Key-chain
- TC — TACACS Configuration

- TRC — Time Range Configuration
- UE — User EXEC
- VC — VLAN Configuration (reached via `vlan database` command)
- v6ACL — IPv6 Access List Configuration
- v6CMC — IPv6 Class-Map Configuration
- v6DP — IPv6 DHCP Pool Configuration

Layer 2 Commands

AAA

Command	Description	Mode ^a
<code>aaa authentication dot1x default</code>	Specifies an authentication method for 802.1x clients.	GC
<code>aaa authentication enable</code>	Defines authentication method lists for accessing higher privilege levels.	GC
<code>aaa authentication login</code>	Defines login authentication.	GC
<code>aaa authorization network default radius</code>	Enables the switch to accept VLAN assignment by the RADIUS server.	GC
<code>aaa ias-user username</code>	Configures IAS users and their attributes. Also changes the mode to aa user config mode.	GC
<code>clear (IAS) aaa ias-users</code>	Deletes all IAS users.	PE
<code>enable authentication</code>	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	LC
<code>enable password</code>	Sets a local password to control access to the normal level.	GC
<code>ip http authentication</code>	Specifies authentication methods for http.	GC
<code>ip https authentication</code>	Specifies authentication methods for https.	GC
<code>login authentication</code>	Specifies the login authentication method list for a remote telnet or console.	LC
<code>password (aaa IAS User Configuration)</code>	Configures a password for a user.	AAA

Command	Description	Mode^a
password (Line Configuration)	Specifies a password on a line.	LC
password (User EXEC)	Specifies a user password	UE
show aaa ias-users	Displays configured IAS users and their attributes.	PE
show authentication methods	Shows information about authentication methods.	PE
show users accounts	Displays information about the local user database.	PE
show users login-history	Displays information about login histories of users.	PE
username	Establishes a username-based authentication system. Optionally allows the specification of an Administrative Profile for a local user.	GC
username unlock	Transfers local user passwords between devices without having to know the passwords.	GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81

Administrative Profiles

Command	Description	Mode^a
admin-profile	Creates an administrative profile.	GC
description (Administrative Profile Config)	Adds a description to an administrative profile.	APC
rule	Adds a rule to an administrative profile.	APC
show admin-profiles	Displays the administrative profiles.	PE
show cli modes	Lists the names of all the CLI modes.	PE
show users	Shows which administrative profiles have been assigned to local user accounts and to show which profiles are active for logged-in users.	PE
username	Optionally allows the specification of an Administrative Profile for a local user.	GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

ACL

Command	Description	Mode ^a
access-list	Creates an Access Control List (ACL) that is identified by the parameter <i>accesslistnumber</i> .	GC
deny permit (IP ACL)	The deny command denies traffic if the conditions defined in the deny statement are matched. The permit command allows traffic if the conditions defined in the permit statement are matched.	ML
ip access-group	Attaches a specified access-control list to an interface.	GC or IC
mac access-group	Attaches a specific MAC Access Control List (ACL) to an interface in the in-bound direction.	GC or IC
mac access-list extended	Creates the MAC Access Control List (ACL) identified by the <i>name</i> parameter.	GC
mac access-list extended rename	Renames the existing MAC Access Control List (ACL) name.	GC
service-acl input	Blocks Link Local Protocol Filtering (LLPF) protocol(s) on a given port.	IC
show service-acl interface	Displays the status of LLPF rules configured on a particular port or on all the ports.	PE
show ip access-lists	Displays an Access Control List (ACL) and all of the rules that are defined for the ACL.	PE
show mac access-list	Displays a MAC access list and all of the rules that are defined for the ACL.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Address Table

Command	Description	Mode ^a
<code>clear mac address-table</code>	Removes any learned entries from the forwarding database.	PE
<code>mac address-table aging-time</code>	Sets the address table aging time.	GC
<code>mac address-table multicast filtering</code>	Enables filtering of Multicast addresses.	GC
<code>mac address-table multicast forbidden address</code>	Forbids adding a specific Multicast address to specific ports.	IC
<code>mac address-table multicast forbidden forward-unregistered</code>	Forbids a port to be a forwarding-unregistered-multicast-addresses port.	IC
<code>mac address-table multicast forward-all</code>	Enables forwarding of all Multicast packets on a port.	IC
<code>mac address-table multicast forward-unregistered</code>	Enables the forwarding of unregistered multicast addresses.	IC
<code>mac address-table multicast static</code>	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.	IC
<code>mac address-table static</code>	Adds a static MAC-layer station source address to the bridge table.	IC
<code>port security</code>	Disables new address learning on an interface.	IC
<code>port security max</code>	Configures the maximum addresses that can be learned on the port while the port is in port security mode.	IC
<code>show mac address-table</code>	Displays dynamically created entries in the bridge-forwarding database.	PE
<code>show mac address-table address</code>	Displays all entries in the bridge-forwarding database for the specified MAC address.	UE or PE
<code>show mac address-table count</code>	Displays the number of addresses present in the Forwarding Database.	PE
<code>show mac address-table dynamic</code>	Displays all entries in the bridge-forwarding database.	UE or PE

Command	Description	Mode ^a
show mac address-table filtering	Displays the Multicast filtering configuration.	PE
show mac address-table interface	Displays the mac forwarding table entries for a specific interface.	UE or PE
show mac address-table multicast	Displays Multicast MAC address table information.	PE
show mac address-table static	Displays statically created entries in the bridge-forwarding database.	PE
show mac address-table vlan	Displays all entries in the bridge-forwarding database for the specified VLAN.	UE or PE
show ports security	Displays the port-lock status.	PE
show ports security addresses	Displays current dynamic addresses in locked ports.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Auto-VoIP

Command	Description	Mode ^a
switchport voice detect auto	Enables the VoIP Profile on all the interfaces of the switch.	GC or IC
show switchport voice	Displays the status of auto-voip on an interface or all interfaces.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

CDP Interoperability

Command	Description	Mode ^a
clear isdp counters	Clears the ISDP counters.	PE
clear isdp table	Clears entries in the ISDP table.	PE
isdp advertise-v2	Enables the sending of ISDP version 2 packets from the device.	GC
isdp enable	Enables ISDP on the switch.	GC or IC

Command	Description	Mode^a
isdp holdtime	Configures the hold time for ISDP packets that the switch transmits.	GC
isdp timer	Sets period of time between sending new ISDP packets.	GC
show isdp	Displays global ISDP settings.	PE
show isdp interface	Displays ISDP settings for the specified interface.	PE
show isdp entry	Displays ISDP entries.	PE
show isdp neighbors	Displays the list of neighboring devices.	PE
show isdp traffic	Displays ISDP statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DHCP L2 Relay

Command	Description	Mode^a
dhcp l2relay (Global Configuration)	Enables the Layer 2 DHCP Relay agent for an interface or globally.	GC or IC
dhcp l2relay circuit-id	Enables user to set the DHCP Option 82 Circuit ID for a VLAN.	GC
dhcp l2relay remote-id	Enables user to set the DHCP Option 82 Remote ID for a VLAN.	GC
dhcp l2relay vlan	Enables the L2 DHCP Relay agent for a set of VLANs.	GC
dhcp l2relay trust	Configures an interface to trust a received DHCP Option 82.	IC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DHCP Management Interface

Command	Description	Mode ^a
<code>release dhcp</code>	Forces the DHCPv4 client to release a leased address.	PE
<code>renew dhcp</code>	Forces the DHCP client to immediately renew an IPv4 address lease.	PE
<code>debug dhcp packet</code>	Displays debug information about DHCPv4 client activities and traces DHCP v4 packets to and from the local DHCPv4 client.	PE
<code>show dhcp lease</code>	Displays IPv4 addresses leased from a DHCP server.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DHCP Snooping

Command	Description	Mode ^a
<code>clear ip dhcp snooping binding</code>	Clears all DHCP Snooping entries.	PE
<code>clear ip dhcp snooping statistics</code>	Clears all DHCP Snooping statistics.	PE
<code>ip dhcp snooping</code>	Enables DHCP snooping globally or on a specific VLAN.	GC or IC
<code>ip dhcp snooping binding</code>	Configures a static DHCP Snooping binding.	GC
<code>ip dhcp snooping database</code>	Configures the persistent location of the DHCP snooping database.	GC
<code>ip dhcp snooping database write-delay</code>	Configures the interval in seconds at which the DHCP Snooping database will be stored in persistent storage.	GC
<code>ip dhcp snooping limit</code>	Controls the maximum rate of DHCP messages.	IC
<code>ip dhcp snooping log-invalid</code>	Enables logging of DHCP messages filtered by the DHCP Snooping application.	IC
<code>ip dhcp snooping trust</code>	Configure a port as trusted for DHCP snooping.	IC

Command	Description	Mode ^a
<code>ip dhcp snooping verify mac-address</code>	Enables the verification of the source MAC address with the client MAC address in the received DHCP message.	GC
<code>show ip dhcp snooping</code>	Displays the DHCP snooping global and per port configuration.	PE
<code>show ip dhcp snooping binding</code>	Displays the DHCP snooping binding entries.	PE
<code>show ip dhcp snooping database</code>	Displays the DHCP snooping configuration related to the database persistence.	PE
<code>show ip dhcp snooping interfaces</code>	Displays the DHCP Snooping status of the interfaces.	PE
<code>show ip dhcp snooping statistics</code>	Displays the DHCP snooping filtration statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Dynamic ARP Inspection

Command	Description	Mode ^a
<code>arp access-list</code>	Creates an ARP ACL.	GC
<code>clear ip arp inspection statistics</code>	Resets the statistics for Dynamic ARP Inspection on all VLANs.	PE
<code>ip arp inspection filter</code>	Configures the ARP ACL to be used for a single VLAN or a range of VLANs to filter invalid ARP packets.	GC
<code>ip arp inspection limit</code>	Configures the rate limit and burst interval values for an interface.	IC
<code>ip arp inspection trust</code>	Configures an interface as trusted for Dynamic ARP Inspection.	IC
<code>ip arp inspection validate</code>	Enables additional validation checks like source MAC address validation, destination MAC address validation or IP address validation on the received ARP packets.	GC
<code>ip arp inspection vlan</code>	Enables Dynamic ARP Inspection on a single VLAN or a range of VLANs.	GC

Command	Description	Mode ^a
permit ip host mac host	Configures a rule for a valid IP address and MAC address combination used in ARP packet validation.	ARPA
show arp access-list	Displays the configured ARP ACLs with the rules.	PE
show ip arp inspection	Displays the Dynamic ARP Inspection configuration.	PE
show ip arp inspection interfaces	Displays the Dynamic ARP Inspection configuration on all the DAI enabled interfaces.	PE
show ip arp inspection vlan	Displays the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

E-mail Alerting

Command	Description	Mode ^a
logging email	Enables e-mail alerting and sets the lowest severity level for which log messages are e-mailed.	GC
logging email urgent	Sets the lowest severity level at which log messages are e-mailed in an urgent manner.	GC
logging traps	Sets the lowest severity level at which SNMP traps are logged.	GC
logging email message-type to-addr	Configures the To address field of the e-mail.	GC
logging email from-addr	Configures the From address of the e-mail.	GC
logging email message-type subject	Configures the subject.	GC
logging email logtime	Configures the value of how frequently the queued messages are sent.	GC
logging email test message-type	Tests whether or not an e-mail is being sent to an SMTP server.	GC

Command	Description	Mode^a
show logging email statistics	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.	PE
clear logging email statistics	Clears the e-mail alerting statistics.	GC
security	Sets the e-mail alerting security protocol.	MSC
mail-server ip-address hostname	Configures the SMTP server IP address and changes the mode to Mail Server Configuration Mode.	GC
port (Mail Server Configuration Mode)	Configures the TCP port to use for communication with the SMTP servers.	MSC
username (Mail Server Configuration Mode)	Configures the username required by the authentication.	MSC
password (Mail Server Configuration Mode)	Configures the password required to authenticate to the e-mail server.	MSC
show mail-server	Displays the configuration of all the mail servers or a particular mail server.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Ethernet Configuration

Command	Description	Mode^a
clear counters	Clears statistics on an interface.	PE
description	Adds a description to an interface.	IC
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	IC
flowcontrol	Configures the flow control on a given interface.	GC
interface	Enters the interface configuration mode to configure parameters for an interface.	GC or IC

Command	Description	Mode^a
interface range	Enters the interface configuration mode to execute a command on multiple ports at the same time.	GC, IC, IR
show interfaces advertise	Displays information about auto negotiation advertisement.	PE
show interfaces configuration	Displays the configuration for all configured interfaces.	UE
show interfaces counters	Displays traffic seen by the physical interface.	UE
show interfaces description	Displays the description for all configured interfaces.	UE
show interfaces detail	Displays the detail for all configured interfaces.	UE
show interfaces status	Displays the status for all configured interfaces.	UE
show statistics	Displays statistics for one port or for the entire switch.	PE
show statistics switchport	Displays detailed statistics for a specific port or for the entire switch.	PE
show storm-control	Displays the storm control configuration.	PE
shutdown	Disables interfaces.	IC
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	IC
storm-control broadcast	Enables Broadcast storm control.	IC
storm-control multicast	Enables the switch to count Multicast packets together with Broadcast packets.	IC
storm-control unicast	Enables Unicast storm control.	IC
switchport protected	Sets the port to Protected mode.	IC
switchport protected name	Configures a name for a protected group.	GC
show switchport protected	Displays protected group/port information.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Ethernet CFM

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

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

GVRP

Command	Description	Mode ^a
<code>clear gvrp statistics</code>	Clears all the GVRP statistics information.	PE
<code>garp timer</code>	Adjusts the GARP application join, leave, and leaveall GARP timer values.	IC
<code>gvrp enable (global)</code>	Enables GVRP globally.	GC
<code>gvrp enable (interface)</code>	Enables GVRP on an interface.	IC
<code>gvrp registration-forbid</code>	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	IC
<code>gvrp vlan-creation-forbid</code>	Enables or disables dynamic VLAN creation.	IC
<code>show gvrp configuration</code>	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.	PE
<code>show gvrp error-statistics</code>	Displays GVRP error statistics.	UE
<code>show gvrp statistics</code>	Displays GVRP statistics.	UE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IGMP Snooping

Command	Description	Mode ^a
<code>ip igmp snooping (global)</code>	In Global Config mode, Enables Internet Group Management Protocol (IGMP) snooping.	GC
<code>ip igmp snooping (interface)</code>	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	IC
<code>ip igmp snooping host-time-out</code>	Configures the host-time-out.	IC
<code>ip igmp snooping leave-time-out</code>	Configures the leave-time-out.	IC
<code>ip igmp snooping mrouter-time-out</code>	Configures the mrouter-time-out.	IC

Command	Description	Mode ^a
<code>show ip igmp snooping groups</code>	Displays Multicast groups learned by IGMP snooping.	UE
<code>show ip igmp snooping interface</code>	Displays IGMP snooping configuration.	PE
<code>show ip igmp snooping mrouter</code>	Displays information on dynamically learned Multicast router interfaces.	PE
<code>ip igmp snooping (VLAN)</code>	In VLAN Config mode, enables IGMP snooping on a particular VLAN or on all interfaces participating in a VLAN.	VC
<code>ip igmp snooping fast-leave</code>	Enables or disables IGMP Snooping fast-leave mode on a selected VLAN.	VC
<code>ip igmp snooping groupmembership-interval</code>	Sets the IGMP Group Membership Interval time on a VLAN.	VC
<code>ip igmp snooping maxresponse</code>	Sets the IGMP Maximum Response time on a particular VLAN.	VC
<code>ip igmp snooping mcertexpiretime</code>	Sets the Multicast Router Present Expiration time.	VC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IGMP Snooping Querier

Command	Description	Mode ^a
<code>ip igmp snooping querier</code>	Enables/disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN.	GC, VC
<code>ip igmp snooping querier election participate</code>	Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.	VC
<code>ip igmp snooping querier query-interval</code>	Sets the IGMP Querier Query Interval time.	GC
<code>ip igmp snooping querier timer expiry</code>	Sets the IGMP Querier timer expiration period.	GC

Command	Description	Mode ^a
<code>ip igmp snooping querier version</code>	Sets the IGMP version of the query that the snooping switch is going to send periodically.	GC
<code>show ip igmp snooping querier</code>	Displays IGMP Snooping Querier information.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IP Addressing

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

Command	Description	Mode ^a
ipv6 enable (Interface Config)	Enables IPv6 on the management interface.	GC
ipv6 enable (OOB Config)	Enables IPv6 operation on the out-of-band interface.	IC
ipv6 gateway (OOB Config)	Configures the address of the IPv6 gateway.	IC
show hosts	Displays the default domain name, a list of name server hosts, static and cached list of host names and addresses.	UE
show ip address-conflict	Displays the status information corresponding to the last detected address conflict.	UE or PE
show ip helper-address	Displays the ip helper addresses configuration.	PE
show ipv6 dhcp interface out-of-band statistics	Displays IPv6 DHCP statistics for the out-of-band interface.	PE
show ipv6 interface out-of-band	Displays the IPv6 out-of-band port configuration.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IPv6 ACL

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

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IPv6 MLD Snooping

Command	Description	Mode ^a
<code>ipv6 mld snooping immediate-leave</code>	Enables or disables MLD Snooping immediate-leave admin mode on a selected interface or VLAN.	IC VC
<code>ipv6 mld snooping groupmembership-interval</code>	Sets the MLD Group Membership Interval time on a VLAN or interface.	IC VC
<code>ipv6 mld snooping maxresponse</code>	Sets the MLD Maximum Response time for an interface or VLAN.	IC or VC
<code>ipv6 mld snooping mrcexpiretime</code>	Sets the Multicast Router Present Expiration time.	IC
<code>ipv6 mld snooping (Global)</code>	Enables MLD Snooping on the system (Global Config Mode).	GC
<code>ipv6 mld snooping (Interface)</code>	Enables MLD Snooping on an interface.	IC
<code>ipv6 mld snooping (VLAN)</code>	Enables MLD Snooping on a particular VLAN and all interfaces participating in that VLAN.	VC
<code>show ipv6 mld snooping</code>	Displays MLD Snooping information.	PE
<code>show ipv6 mld snooping groups</code>	Displays the MLD Snooping entries in the MFDB table.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IPv6 MLD Snooping Querier

Command	Description	Mode ^a
<code>ipv6 mld snooping querier</code>	Enables MLD Snooping Querier on the system or on a VLAN.	GC or VC
<code>ipv6 mld snooping querier address</code>	Sets the global MLD Snooping Querier address on the system or on a VLAN.	GC or VC
<code>ipv6 mld snooping querier election participate</code>	Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.	VC

Command	Description	Mode^a
<code>ipv6 mld snooping querier query-interval</code>	Sets the MLD Querier Query Interval time.	GC
<code>ipv6 mld snooping querier timer expiry</code>	Sets the MLD Querier timer expiration period.	GC
<code>show ipv6 mld snooping querier</code>	Displays MLD Snooping Querier information.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IP Source Guard

Command	Description	Mode^a
<code>ip verify source</code>	Enables filtering of IP packets matching the source IP address.	IC
<code>ip verify source port-security</code>	Enables filtering of IP packets matching the source IP address and the source MAC address.	IC
<code>ip verify binding</code>	Configures static bindings.	GC
<code>show ip verify interface</code>	Displays the IPSPG interface configuration.	PE
<code>show ip verify source interface</code>	Displays the bindings configured on a particular interface.	PE
<code>show ip source binding</code>	Displays all bindings (static and dynamic).	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

iSCSI Optimization

Link Dependency

Command	Description	Mode ^a
iscsi aging time	Sets aging time for iSCSI sessions.	GC
iscsi cos	Sets the quality of service profile that will be applied to iSCSI flows.	GC
iscsi enable	Enables Global Configuration mode command globally enables iSCSI awareness.	GC
iscsi target port	Configures an iSCSI target port (optionally configures target port address and name).	GC
show iscsi	Displays the iSCSI settings.	PE
show iscsi sessions	Displays the iSCSI sessions.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Command	Description	Mode ^a
action	Indicates if the link-dependency group should mirror or invert the status of the depended on interfaces.	LD
link-dependency group	Enters the link-dependency mode to configure a link-dependency group.	GC
add gigabitethernet	Adds member gigabit Ethernet port(s) to the dependency list.	LD
add tengigabitethernet	Adds member ten gigabit Ethernet port(s) to the dependency list.	LD
add port-channel	Adds member port-channels to the dependency list.	LD
depends-on	Adds the dependent Ethernet ports or port channels list.	LD
show link-dependency	Shows the link dependencies configured on a particular group.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

LLDP

Command	Description	Mode ^a
<code>clear lldp remote-data</code>	Deletes all data from the remote data table.	PE
<code>clear lldp statistics</code>	Resets all LLDP statistics.	PE
<code>lldp notification</code>	Enables remote data change notifications.	IC
<code>lldp notification-interval</code>	Limits how frequently remote data change notifications are sent.	GC
<code>lldp receive</code>	Enables the LLDP receive capability.	IC
<code>lldp timers</code>	Sets the timing parameters for local data transmission on ports enabled for LLDP.	GC
<code>lldp transmit</code>	Enables the LLDP advertise capability.	IC
<code>lldp transmit-mgmt</code>	Specifies that transmission of the local system management address information in the LLDPDUs is included.	IC
<code>lldp transmit-tlv</code>	Specifies which optional TLVs in the 802.1AB basic management set will be transmitted in the LLDPDUs.	IC
<code>show lldp</code>	Displays the current LLDP configuration summary.	PE
<code>show lldp interface</code>	Displays the current LLDP interface state.	PE
<code>show lldp local-device</code>	Displays the LLDP local data.	PE
<code>show lldp remote-device</code>	Displays the current LLDP remote data.	PE
<code>show lldp statistics</code>	Displays the current LLDP traffic statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Multicast VLAN Registration

Command	Description	Mode ^a
<code>mvr</code>	Enables MVR.	GC or IC
<code>mvr group</code>	Adds an MVR membership group.	GC
<code>mvr mode</code>	Changes the MVR mode type.	GC

Command	Description	Mode^a
mvr querytime	Sets the MVR query response time.	GC
mvr vlan	Sets the MVR multicast VLAN.	GC
mvr immediate	Enables MVR Immediate Leave mode.	IC
mvr type	Sets the MVR port type.	IC
mvr vlan group	Use to participate in the specific MVR group.	IC
show mvr	Displays global MVR settings.	PE
show mvr members	Displays the MVR membership groups allocated.	PE
show mvr interface	Displays the MVR enabled interface configuration.	PE
show mvr traffic	Displays global MVR statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Port Channel

Command	Description	Mode^a
channel-group	Associates a port with a port-channel.	IC
interface port-channel	Enters the interface configuration mode of a specific port-channel.	GC
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	GC
hashing-mode	Sets the hashing algorithm on trunk ports.	IC (port-channel)
lACP port-priority	Configures the priority value for physical ports.	IC
lACP system-priority	Configures the system LACP priority.	GC
lACP timeout	Assigns an administrative LACP timeout.	IC
port-channel min-links	Sets the minimum number of links that must be up in order for the port channel interface to be declared up.	IC
show interfaces port-channel	Displays port-channel information.	PE

Command	Description	Mode ^a
<code>show lacp</code>	Displays LACP information for ports.	PE
<code>show statistics port-channel</code>	Displays port-channel statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Port Monitor

Command	Description	Mode ^a
<code>monitor session</code>	Configures a port monitoring session.	GC
<code>show monitor session</code>	Displays the port monitoring status.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

QoS

Command	Description	Mode ^a
<code>assign-queue</code>	Modifies the queue ID to which the associated traffic stream is assigned.	PCMC
<code>class</code>	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.	PMC
<code>class-map</code>	Defines a new DiffServ class of type <i>match-all</i> , <i>match-any</i> , or <i>match-access-group</i> . For now, only <i>match-all</i> is available in the CLI.	GC
<code>class-map rename</code>	Changes the name of a DiffServ class.	GC
<code>classofservice dot1p-mapping</code>	Maps an 802.1p priority to an internal traffic class for a switch.	GC or IC
<code>classofservice ip-dscp-mapping</code>	Maps an IP DSCP value to an internal traffic class.	GC
<code>classofservice trust</code>	Sets the class of service trust mode of an interface.	GC or IC
<code>conform-color</code>	Specifies for each outcome, the only possible actions are drop, setdscp-transmit, set-prec-transmit, or transmit.	PCMC

Command	Description	Mode^a
<code>cos-queue min-bandwidth</code>	Specifies the minimum transmission bandwidth for each interface queue.	GC or IC
<code>cos-queue random-detect</code>	Configures WRED queue management policy on an interface CoS queue.	GC or IC
<code>cos-queue strict</code>	Activates the strict priority scheduler mode for each specified queue.	GC or IC
<code>diffserv</code>	Sets the DiffServ operational mode to active.	GC
<code>drop</code>	Use the drop policy-class-map configuration command to specify that all packets for the associated traffic stream are to be dropped at ingress.	PCMC
<code>mark cos</code>	Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header.	PCMC
<code>mark ip-dscp</code>	Marks all packets for the associated traffic stream with the specified IP DSCP value.	PCMC
<code>mark ip-precedence</code>	Marks all packets for the associated traffic stream with the specified IP precedence value.	PCMC
<code>match class-map</code>	Adds add to the specified class definition the set of match conditions defined for another class.	CMC
<code>match cos</code>	Adds to the specified class definition a match condition for the Class of Service value.	CMC
<code>match destination-address mac</code>	Adds to the specified class definition a match condition based on the destination MAC address of a packet.	CMC
<code>match dstip</code>	Adds to the specified class definition a match condition based on the destination IP address of a packet.	CMC
<code>match dstip6</code>	Adds to the specified class definition a match condition based on the destination IPv6 address of a packet.	v6CMC

Command	Description	Mode^a
<code>match dstl4port</code>	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.	CMC
<code>match ethertype</code>	Adds to the specified class definition a match condition based on the value of the ethertype.	CMC
<code>match ip6flowlbl</code>	Adds to the specified class definition a match condition based on the IPv6 flow label of a packet.	v6CMC
<code>match ip dscp</code>	Adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet.	CMC
<code>match ip precedence</code>	Adds to the specified class definition a match condition based on the value of the IP.	CMC
<code>match ip tos</code>	Adds to the specified class definition a match condition based on the value of the IP TOS field in a packet.	CMC
<code>match protocol</code>	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.	CMC
<code>match source-address mac</code>	Adds to the specified class definition a match condition based on the source MAC address of the packet.	CMC
<code>match srcip</code>	Adds to the specified class definition a match condition based on the source IP address of a packet.	CMC
<code>match srcip6</code>	Adds to the specified class definition a match condition based on the source IPv6 address of a packet.	v6CMC
<code>match srcl4port</code>	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.	CMC

Command	Description	Mode^a
match vlan	Adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field.	CMC
mirror	Mirrors all the data that matches the class defined to the destination port specified.	PCMC
police-simple	Establishes the traffic policing style for the specified class.	PCMC
policy-map	Establishes a new DiffServ policy or enters policy map configuration mode.	GC
random-detect queue-parns	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.	GC, IC, or IR
random-detect exponential-weighting-constant	Configures the decay in the calculation of the average queue size user for WRED on an interface or all interfaces.	GC, IC, or IR
redirect	Specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).	PCMC
service-policy	Attaches a policy to an interface in a particular direction.	GC or IC
show class-map	Displays all configuration information for the specified class.	PE
show classofservice dot1p-mapping	Displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.	PE
show classofservice ip-dscp-mapping	Displays the current IP DSCP mapping to internal traffic classes for a specific interface.	PE
show classofservice trust	Displays the current trust mode setting for a specific interface.	PE
show diffserv	Displays the DiffServ General Status information.	PE

Command	Description	Mode^a
<code>show diffserv service interface</code>	Displays policy service information for the specified interface and direction.	PE
<code>show diffserv service interface port-channel</code>	Displays policy service information for the specified interface and direction.	PE
<code>show diffserv service brief</code>	Displays all interfaces in the system to which a DiffServ policy has been attached.	PE
<code>show interfaces cos-queue</code>	Displays the class-of-service queue configuration for the specified interface.	PE
<code>show interfaces random-detect</code>	Displays the WRED policy on an interface.	PE
<code>show policy-map</code>	Displays all configuration information for the specified policy.	PE
<code>show policy-map interface</code>	Displays policy-oriented statistics information for the specified interface and direction.	PE
<code>show service-policy</code>	Displays a summary of policy-oriented statistics information for all interfaces.	PE
<code>traffic-shape</code>	Specifies the maximum transmission bandwidth limit for the interface as a whole.	GC or IC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Radius

Command	Description	Mode^a
<code>aaa accounting dot1x default start-stop</code>	Creates an accounting method list	GC
<code>accounting</code>	Applies an accounting method to a line config.	LC
<code>acct-port</code>	Sets the port that connects to the RADIUS accounting server.	R
<code>auth-port</code>	Sets the port number for authentication requests of the designated radius server.	R

Command	Description	Mode^a
deadtime	Improves Radius response times when a server is unavailable by causing the unavailable server to be skipped.	R
debug aaa accounting	Enables debugging for accounting.	PE
key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	R
msgauth	Enables the message authenticator attribute to be used for the RADIUS Authenticating server being configured.	R
name (RADIUS server)	Assigns a name to a RADIUS server.	R
primary	Specifies that a configured server should be the primary server in the group of authentication servers which have the same server name.	R
priority	Specifies the order in which the servers are to be used, with 0 being the highest priority.	R
radius-server attribute 4	Sets the network access server (NAS) IP address for the RADIUS server.	GC
radius-server deadtime	Improves RADIUS response times when servers are unavailable. Causes the unavailable servers to be skipped.	GC
radius-server host	Specifies a RADIUS server host.	GC
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	GC
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	GC
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	GC
radius-server timeout	Sets the interval for which a switch waits for a server host to reply.	GC
retransmit	Specifies the number of times the software searches the list of RADIUS server hosts before stopping the search.	R

Command	Description	Mode ^a
<code>show aaa servers</code>	Displays the list of configured RADIUS servers and the values configured for the global parameters of the RADIUS client.	UE or PE
<code>show accounting methods</code>	Displays the configured accounting method lists.	PE
<code>show radius statistics</code>	Shows the statistics for an authentication or accounting server.	UE or PE
<code>source-ip</code>	Specifies the source IP address to be used for communication with RADIUS servers.	R
<code>timeout</code>	Sets the timeout value in seconds for the designated radius server.	R
<code>usage</code>	Specifies the usage type of the server.	R

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Spanning Tree

Command	Description	Mode ^a
<code>clear spanning-tree detected-protocols</code>	Restarts the protocol migration process on all interfaces or on the specified interface.	PE
<code>exit (mst)</code>	Exits the MST configuration mode and applies configuration changes.	MC
<code>instance (mst)</code>	Maps VLANs to an MST instance.	MC
<code>name (mst)</code>	Defines the MST configuration name.	MC
<code>revision (mst)</code>	Defines the configuration revision number.	MC
<code>show spanning-tree</code>	Displays spanning tree configuration.	PE
<code>show spanning-tree summary</code>	Displays spanning tree settings and parameters for the switch.	PE
<code>spanning-tree</code>	Enables spanning-tree functionality.	GC
<code>spanning-tree auto-portfast</code>	Sets the port to auto portfast mode.	IC
<code>spanning-tree bpdud flooding</code>	Allows flooding of BPDUs received on nonspanning-tree ports to all other nonspanning-tree ports.	GC

Command	Description	Mode^a
spanning-tree bpduprotection	Enables BPDU protection on a switch.	GC
spanning-tree cost	Configures the spanning tree path cost for a port.	IC
spanning-tree disable	Disables spanning tree on a specific port.	IC
spanning-tree forward-time	Configures the spanning tree bridge forward time.	GC
spanning-tree guard	Selects whether loop guard or root guard is enabled on an interface.	IC
spanning-tree loopguard	Enables loop guard on all ports.	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age.	GC
spanning-tree max-hops	Sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree.	GC
spanning-tree mode	Configures the spanning tree protocol.	GC
spanning-tree mst configuration	Enables configuring an MST region by entering the multiple spanning-tree (MST) mode.	GC
spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.	IC
spanning-tree mst port-priority	Configures port priority.	IC
spanning-tree mst priority	Configures the switch priority for the specified spanning tree instance.	GC
spanning-tree portfast	Enables PortFast mode.	IC
spanning-tree portfast bpdudfilter default	Discards BPDUs received on spanningtree ports in portfast mode.	GC
spanning-tree portfast default	Enables Portfast mode on all ports.	GC
spanning-tree port-priority	Configures port priority.	IC
spanning-tree priority	Configures the spanning tree priority.	GC

Command	Description	Mode ^a
<code>spanning-tree tenguard</code>	Prevents a port from propagating topology change notifications.	IC
<code>spanning-tree transmit hold-count</code>	Set the maximum number of BPDUs that a bridge is allowed to send within a hello time window (2 seconds).	GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

TACACS+

Command	Description	Mode ^a
<code>key</code>	Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server.	TC
<code>port</code>	Specifies a server port number.	TC
<code>priority</code>	Specifies the order in which servers are used.	TC
<code>show tacacs</code>	Displays TACACS+ server settings and statistics.	PE
<code>tacacs-server host</code>	Specifies a TACACS+ server host.	GC
<code>tacacs-server key</code>	Sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon.	GC
<code>tacacs-server timeout</code>	Sets the interval for which the switch waits for a server host to reply.	GC
<code>timeout</code>	Specifies the timeout value in seconds.	TC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

VLAN

Command	Description	Mode ^a
<code>dvlan-tunnel ethertype</code>	Configures the EtherType for the interface.	GC
<code>interface vlan</code>	Enters the VLAN interface configuration mode.	GC
<code>interface range vlan</code>	Enters the interface configuration mode to configure multiple VLANs.	GC

Command	Description	Mode^a
<code>mode dvlan-tunnel</code>	Enables Double VLAN tunneling on the specified interface.	IC
<code>name (VLAN Configuration)</code>	Configures a name to a VLAN.	IC
<code>private-vlan</code>	Defines a private VLAN association between the primary and secondary VLANs.	VC
<code>protocol group</code>	Attaches a <i>vlanid</i> to the protocol-based VLAN identified by <i>groupid</i> .	VC
<code>protocol vlan group</code>	Adds the physical unit/slot/port interface to the protocol-based VLAN identified by <i>groupid</i> .	IC
<code>protocol vlan group all</code>	Adds all physical unit/slot/port interfaces to the protocol-based VLAN identified by <i>groupid</i> .	GC
<code>show dvlan-tunnel</code>	Displays all interfaces enabled for Double VLAN Tunneling.	PE
<code>show dvlan-tunnel interface</code>	Displays detailed information about Double VLAN Tunneling for the specified interface.	PE
<code>show interfaces switchport</code>	Displays switchport configuration.	PE, IC
<code>show port protocol</code>	Displays the Protocol-Based VLAN information for either the entire system or for the indicated group.	PE
<code>show vlan</code>	Displays detailed information, including interface information and dynamic vlan type, for a specific VLAN.	PE
<code>show vlan association mac</code>	Displays the VLAN associated with a specific configured MAC address.	PE
<code>show vlan association subnet</code>	Displays the VLAN associated with a specific configured IP subnet.	PE
<code>show vlan private-vlan</code>		
<code>switchport access vlan</code>	Configures the VLAN ID when the interface is in access mode.	IC
<code>switchport forbidden vlan</code>	Forbids adding specific VLANs to a port.	IC

Command	Description	Mode^a
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	IC
switchport general allowed vlan	Adds or removes VLANs from a port in General mode.	IC
switchport general ingress-filtering disable	Disables port ingress filtering.	IC
switchport general pvid	Configures the PVID when the interface is in general mode.	IC
switchport mode	Configures the VLAN membership mode of a port.	IC
switchport mode private-vlan	Defines a private VLAN association for an isolated or community port or a mapping for a promiscuous port.	IC
switchport private-vlan	Defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.	IC
switchport trunk	Adds or removes VLANs from a trunk port.	IC
vlan	Creates a VLAN.	VC
vlan (Global Config)	Configures a VLAN.	GC
vlan association mac	Associates a MAC address to a VLAN.	VC
vlan association subnet	Associates an IP subnet to a VLAN.	VC
vlan database	Enters the VLAN database configuration mode.	GC
vlan makestatic	Changes a dynamically created VLAN to a static VLAN.	VC
vlan protocol group	Adds protocol-based VLAN groups to the system.	GC
vlan protocol group add protocol	Adds a protocol to the protocol-based VLAN identified by <i>groupid</i> .	GC
vlan protocol group name	Adds a group name to the protocol-based VLAN identified by <i>groupid</i> .	GC

Command	Description	Mode ^a
<code>vlan protocol group remove</code>	Removes the protocol-base VLAN group identified by <i>groupid</i> .	GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

802.1x

Command	Description	Mode ^a
<code>dot1x dynamic-vlan enable</code>	Enables the capability of creating VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.	GC
<code>dot1x initialize</code>	Begins the initialization sequence on the specified port.	PE
<code>dot1x mac-auth-bypass</code>	Enables MAB on an interface.	IC
<code>dot1x max-req</code>	Sets the maximum number of times the switch sends an EAP-request frame to the client before restarting the authentication process.	IC
<code>dot1x max-users</code>	Sets the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port.	IC
<code>dot1x port-control</code>	Enables manual control of the authorization state of the port.	IC
<code>dot1x re-authenticate</code>	Manually initiates a re-authentication of all 802.1x-enabled ports or a specified 802.1X enabled port.	PE
<code>dot1x reauthentication</code>	Enables periodic re-authentication of the client.	IC
<code>dot1x system-auth-control monitor</code>	Enables 802.1X globally.	GC
<code>dot1x timeout guest-vlan-period</code>	Sets the number of seconds that the switch waits before authorizing the client if the client is a dot1x unaware client.	IC
<code>dot1x timeout quiet-period</code>	Sets the number of seconds the switch remains in the quiet state following a failed authentication attempt.	IC

Command	Description	Mode^a
<code>dot1x timeout re-authperiod</code>	Sets the number of seconds between re-authentication attempts.	IC
<code>dot1x timeout server-timeout</code>	Sets the number of seconds the switch waits for a response from the authentication server before resending the request.	IC
<code>dot1x timeout supp-timeout</code>	Sets the number of seconds the switch waits for a response to an EAP-request frame from the client before retransmitting the request.	IC
<code>dot1x timeout tx-period</code>	Sets the number of seconds the switch waits for a response to an EAP-request/identify frame from the client before resending the request.	IC
<code>show dot1x</code>	Displays 802.1X status for the switch or the specified interface.	PE
<code>show dot1x authentication-history</code>	Displays the dot1x authentication events and information during successful and unsuccessful dot1x authentication processes.	PE
<code>show dot1x clients</code>	Displays detailed information about the users who have successfully authenticated on the system or on a specified port.	PE
<code>show dot1x interface</code>	Shows the status of MAC Authentication Bypass.	PE
<code>show dot1x interface statistics</code>	Displays 802.1X statistics for the specified interface.	PE
<code>show dot1x users</code>	Displays active 802.1X authenticated users for the switch.	PE
<code>clear dot1x authentication-history</code>	Clears the authentication history table captured during successful and unsuccessful authentication.	PE
<code>dot1x guest-vlan</code>	Sets the guest VLAN on a port.	IC
<code>dot1x unauth-vlan</code>	Specifies the unauthenticated VLAN on a port.	IC
<code>show dot1x advanced</code>	Displays 802.1X advanced features for the switch or specified interface.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Data Center Technology Commands

Data Center Bridging Commands

Command	Description	Mode ^a
<code>datacenter-bridging</code>	Enters the Data Center Bridging mode.	IC
<code>lldp dcbx version</code>	Enables the switch to support a specific version of the Data Center Bridging Capability Exchange (DCBX) protocol or to detect the peer version and match it.	GC
<code>lldp tlv-select dcbx</code>	Sends specific DCBX TLVs if LLDP is enabled to transmit on the given interface. If no parameter is given, all DCBX TLVs are enabled for transmission.	IC, GC
<code>lldp dcbx port-role</code>	Configures the port role to manual, auto-upstream, auto-downstream and configuration source.	IC
<code>show lldp tlv-select</code>	Displays the per interface TLV configuration.	PE
<code>show lldp dcbx</code>	Displays the per interface DCBX configuration and status.	PE

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

FIP Snooping Commands

Command	Description	Mode ^a
<code>feature fip-snooping</code>	Globally enables Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch.	GC
<code>fip-snooping enable</code>	Enables snooping of FIP packets on the configured VLANs.	VC
<code>fip-snooping fc-map</code>	Configures the FP-MAP value on a VLAN.	VC
<code>fip-snooping port-mode</code>	Configure the interface that is connected toward FCF.	IC
<code>show fip-snooping</code>	Displays information about the global FIP snooping configuration and status.	UE, PE

Command	Description	Mode^a
<code>show fip-snooping enode</code>	Displays information about the interfaces connected to ENodes	UE, PE
<code>show fip-snooping fcf</code>	Displays information about the interfaces connected to FCFs.	UE, PE
<code>show fip-snooping sessions</code>	Displays information about the active FIP snooping sessions.	UE, PE
<code>show fip-snooping statistics</code>	Displays the statistics of the FIP packets snooped in the VLAN or on an interface.	UE, PE
<code>show fip-snooping vlan</code>	Displays the FCoE VLANs information and, additionally, the FIP snooping port status when optional argument is specified.	UE, PE
<code>clear fip-snooping statistics</code>	Clears the FIP Snooping statistics in the supplied VLAN or on a supplied interface.	UE, PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Priority Flow Control Commands

Command	Description	Mode^a
<code>priority-flow-control mode</code>	Enables Priority-Flow-Control (PFC) on an interface.	DCB
<code>priority-flow-control priority</code>	Enables the priority group for lossless behavior (PFC enabled).	DCB
<code>clear priority-flow-control statistics</code>	Clears all or interface Priority-Flow-Control statistics.	PE
<code>show interfaces priority-flow-control</code>	Displays the global or interface priority flow control status and statistics.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Layer 3 Commands

ARP (IPv4)

Command	Description	Mode ^a
<code>arp</code>	Creates an Address Resolution Protocol (ARP) entry.	GC
<code>arp cachesize</code>	Configures the maximum number of entries in the ARP cache.	GC
<code>arp dynamicrenew</code>	Enables the ARP component to automatically renew dynamic ARP entries when they age out.	GC
<code>arp purge</code>	Causes the specified IP address to be removed from the ARP cache.	PE
<code>arp resptime</code>	Configures the ARP request response timeout.	GC
<code>arp retries</code>	Configures the ARP count of maximum request for retries.	GC
<code>arp timeout</code>	Configures the ARP entry age-out time.	GC
<code>clear arp-cache</code>	Removes all ARP entries of type dynamic from the ARP cache.	PE
<code>clear arp-cache management</code>	Removes all entries from the ARP cache learned from the management port.	PE
<code>ip local-proxy-arp</code>	Enables proxying of ARP requests.	IC
<code>ip proxy-arp</code>	Enables proxy ARP on a router interface.	IC
<code>show arp</code>	Displays the Address Resolution Protocol (ARP) cache.	PE
<code>show arp brief</code>	Displays the brief Address Resolution Protocol (ARP) table information.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DHCP Server and Relay Agent (IPv4)

Command	Description	Mode ^a
<code>ip dhcp pool</code>	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.	GC
<code>bootfile</code>	Sets the name of the image for the DHCP client to load.	DP
<code>clear ip dhcp binding</code>	Removes automatic DHCP server bindings.	PE
<code>clear ip dhcp conflict</code>	Removes DHCP server address conflicts.	PE
<code>client-identifier</code>	Identifies a a Microsoft® DHCP client to be manually assigned an address.	DP
<code>client-name</code>	Specifies the host name of a DHCP client.	DP
<code>default-router</code>	Sets the IPv4 address of one or more routers for the DHCP client to use.	DP
<code>dns-server (IP DHCP Pool Config)</code>	Sets the IPv4 DNS server address which is provided to a DHCP client by the DHCP server.	DP
<code>domain-name (IP DHCP Pool Config)</code>	Sets the DNS domain name which is provided to a DHCP client by the DHCP server.	DP
<code>hardware-address</code>	Specifies the MAC address of a client to be manually assigned an address.	DP
<code>host</code>	Specifies a manual binding for a DHCP client host.	DP
<code>ip dhcp bootp automatic</code>	Enables automatic BOOTP address assignments.	GC
<code>ip dhcp conflict logging</code>	Enables DHCP address conflict detection.	GC
<code>ip dhcp excluded-address</code>	Excludes one or more DHCP addresses from automatic assignment.	GC
<code>ip dhcp ping packets</code>	Configures the number of pings sent to detect if an address is in use prior to assigning an address from the DHCP pool.	GC
<code>lease</code>	Sets the period for which a dynamically assigned DHCP address is valid.	DP

Command	Description	Mode^a
netbios-name-server	Configures the IPv4 address of the Windows® Internet Naming Service (WINS) for a Microsoft DHCP client.	DP
netbios-node-type	Sets the NetBIOS node type for a Microsoft DHCP client.	DP
network	Defines a pool of IPv4 addresses for distributing to clients.	DP
next-server	Sets the IPv4 address of the TFTP server to be used during auto-install.	DP
option	Supplies arbitrary configuration information to a DHCP client.	DP
service dhcp	Enables local IPv4 DHCP server on the switch.	GC
ntp	Sets the IPv4 address of the NTP server to be used for time synchronization of the client.	DP
show ip dhcp binding	Displays the configured DHCP bindings.	PE
show ip dhcp conflict	Displays DHCP address conflicts for all relevant interfaces or a specified interface.	PE
show ip dhcp global configuration	Displays the DHCP global configuration.	PE
show ip dhcp pool	Displays the configured DHCP pool or pools.	UE or PE
show ip dhcp server statistics	Displays the DHCP server binding and message counters.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DHCPv6

Command	Description	Mode^a
clear ipv6 dhcp	Clears DHCPv6 statistics for all interfaces or for a specific interface.	PE
dns-server (IPv6 DHCP Pool Config)	Sets the IPv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP

Command	Description	Mode ^a
domain-name (IPv6 DHCP Pool Config)	Sets the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP
ipv6 dhcp pool	Enters IPv6 DHCP Pool Configuration mode.	GC
ipv6 dhcp relay	Configures an interface for DHCPv6 Relay functionality.	IC
ipv6 dhcp server	Configures DHCPv6 server functionality on an interface.	IC
prefix-delegation	Defines Multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.	v6DP
service dhcpv6	Enables DHCPv6 configuration on the router.	GC
show ipv6 dhcp	Displays the DHCPv6 server name and status.	PE
show ipv6 dhcp binding	Displays the configured DHCP pool.	PE
show ipv6 dhcp interface (User EXEC)	Displays DHCPv6 information for all relevant interfaces or a specified interface.	UE PE
show ipv6 dhcp pool	Displays the configured DHCP pool.	PE
show ipv6 dhcp statistics	Displays the DHCPv6 server name and status.	UE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

DVMRP

Command	Description	Mode ^a
ip dvmrp	Sets the administrative mode of DVMRP in the router to active.	GC IC
ip dvmrp metric	Configures the metric for an interface.	IC
show ip dvmrp	Displays the system-wide information for DVMRP.	PE
show ip dvmrp interface	Displays the interface information for DVMRP on the specified interface.	PE
show ip dvmrp neighbor	Displays the neighbor information for DVMRP.	PE

Command	Description	Mode^a
<code>show ip dvmrp nexthop</code>	Displays the next hop information on outgoing interfaces for routing multicast datagrams.	PE
<code>show ip dvmrp prune</code>	Displays the table that lists the router's upstream prune information.	PE
<code>show ip dvmrp route</code>	Displays the multicast routing information for DVMRP.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IGMP

Command	Description	Mode^a
<code>ip igmp</code>	Sets the administrative mode of IGMP in the system to active.	GC
<code>ip igmp last-member-query-count</code>	Sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.	IC
<code>ip igmp last-member-query-interval</code>	Configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.	IC
<code>ip igmp query-interval</code>	Configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.	IC
<code>ip igmp query-max-response-time</code>	Configures the maximum response time interval for the specified interface.	IC
<code>ip igmp robustness</code>	Configures the robustness that allows tuning of the interface.	IC
<code>ip igmp startup-query-count</code>	Sets the number of queries sent out on startup—at intervals equal to the startup query interval for the interface.	IC
<code>ip igmp startup-query-interval</code>	Sets the interval between general queries sent at startup on the interface.	IC

Command	Description	Mode ^a
ip igmp version	Configures the version of IGMP for an interface.	IC
show ip igmp	Displays system-wide IGMP information.	PE
show ip igmp groups	Displays the registered multicast groups on the interface.	PE
show ip igmp interface	Displays the IGMP information for the specified interface.	PE
show ip igmp membership	Displays the list of interfaces that have registered in the multicast group.	PE
show ip igmp interface stats	Displays the IGMP statistical information for the interface.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IGMP Proxy

Command	Description	Mode ^a
ip igmp-proxy	Enables the IGMP Proxy on the router.	IC
ip igmp-proxy reset-status	Resets the host interface status parameters of the IGMP Proxy router.	IC
ip igmp-proxy unsolicited-report-interval	Sets the unsolicited report interval for the IGMP Proxy router.	IC
show ip igmp-proxy	Displays a summary of the host interface status parameters.	PE
show ip igmp-proxy interface	Displays a detailed list of the host interface status parameters.	PE
show ip igmp-proxy groups	Displays a table of information about multicast groups that IGMP Proxy reported.	PE
show ip igmp-proxy groups detail	Displays complete information about multicast groups that IGMP Proxy has reported.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IP Helper/DHCP Relay

Command	Description	Mode ^a
<code>bootpdhcprelay maxhopcount</code>	Configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.	GC
<code>bootpdhcprelay minwaittime</code>	Configures the minimum wait time in seconds for BootP/DHCP Relay on the system.	GC
<code>clear ip helper statistics</code>	Resets (to 0) the statistics displayed in <code>show ip helper statistics</code> .	PE
<code>ip dhcp relay information check</code>	Enables DHCP Relay to check that the relay agent information option in forwarded BOOTREPLY messages is valid.	GC
<code>ip dhcp relay information check-reply</code>	Enables DHCP Relay to check that the relay agent information option in forwarded BOOTREPLY messages is valid.	IC
<code>ip dhcp relay information option</code>	Enables the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system (also called option 82).	GC
<code>ip dhcp relay information option-insert</code>	Enables the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the interface (also called option 82).	GC
<code>ip helper-address (global configuration)</code>	Configures the relay of certain UDP broadcast packets received on any interface.	GC
<code>ip helper-address (interface configuration)</code>	Configures the relay of certain UDP broadcast packets received on a specific interface.	IC
<code>ip helper enable</code>	Enables relay of UDP packets.	GC
<code>show ip helper-address</code>	Displays the IP helper address configuration.	PE
<code>show ip dhcp relay</code>	Displays the BootP/DHCP Relay information.	UE or PE
<code>show ip helper statistics</code>	Displays the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IP Routing

Command	Description	Mode ^a
encapsulation	Configures the link layer encapsulation type for the packet.	IC
ip address	Configures an IP address on an interface.	IC
ip mtu	Sets the IP Maximum Transmission Unit (MTU) on a routing interface.	IC
ip netdirbroadcast	Enables the forwarding of network-directed broadcasts.	IC
ip route	Configures a static route. Use the no form of the command to delete the static route.	GC
ip route default	Configures the default route. Use the no form of the command to delete the default route.	GC
ip route distance	Sets the default distance (preference) for static routes.	GC
ip routing	Globally enables IPv4 routing on the router.	GC
show ip brief	Displays all the summary information of the IP.	PE
show ip interface	Displays all pertinent information about the IP interface.	PE
show ip protocols	Displays the parameters and current state of the active routing protocols.	PE
show ip route	Displays the routing table.	PE
show ip route preferences	Displays detailed information about the route preferences.	PE
show ip route summary	Shows the number of all routes, including best and non-best routes.	PE
show ip traffic	Displays IP statistical information.	UE or PE
show ip vlan	Displays the VLAN routing information for all VLANs with routing enabled.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IPv6 Routing

Command	Description	Mode ^a
<code>clear ipv6 neighbors</code>	Clears all entries in the IPv6 neighbor table or an entry on a specific interface.	PE
<code>clear ipv6 statistics</code>	Clears IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces.	PE
<code>ipv6 address</code>	Configures an IPv6 address on an interface (including tunnel and loopback interfaces).	IC
<code>ipv6 enable</code>	Enables IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address.	IC
<code>ipv6 hop-limit</code>	Configures the hop limit used in IPv6 PDUs originated by the router.	GC
<code>ipv6 host</code>	Defines static host name-to- ipv6 address mapping in the host cache.	GC
<code>ipv6 mld last-member-query-count</code>	Sets the number of listener-specific queries sent before the router assumes that there are no local members on the interface.	IC (VC)
<code>ipv6 mld last-member-query-interval</code>	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)
<code>ipv6 mld-proxy</code>	Enables MLD Proxy on the router.	IC
<code>ipv6 mld-proxy reset-status</code>	Resets the host interface status parameters of the MLD Proxy router.	IC
<code>ipv6 mld-proxy unsolicit-rprt-interval</code>	Sets the unsolicited report interval for the MLD Proxy router.	IC
<code>ipv6 mld query-interval</code>	Sets the MLD router's query interval for the interface.	IC
<code>ipv6 mld query-max-response-time</code>	Sets MLD querier's maximum response time for the interface.	IC

Command	Description	Mode^a
ipv6 mld router	Enables MLD in the router in global configuration mode and for a specific interface in interface configuration mode.	GC or IC
ipv6 mtu	Sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface.	IC
ipv6 nd dad attempts	Sets the number of duplicate address detection probes transmitted while doing neighbor discovery.	IC
ipv6 nd managed-config-flag	Sets the managed address configuration flag in router advertisements.	IC
ipv6 nd ns-interval	Sets the interval between router advertisements for advertised neighbor solicitations.	IC
ipv6 nd other-config-flag	Sets the other stateful configuration flag in router advertisements sent from the interface.	IC
ipv6 nd prefix	Sets the IPv6 prefixes to include in the router advertisement.	IC
ipv6 nd ra-interval	Sets the transmission interval between router advertisements.	IC
ipv6 nd ra-lifetime	Sets the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.	IC
ipv6 nd reachable-time	Sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.	IC
ipv6 nd suppress-ra	Suppresses router advertisement transmission on an interface.	IC
ipv6 route	Configures an IPv6 static route	GC
ipv6 route distance	Sets the default distance (preference) for static routes.	GC
ipv6 unicast-routing	Enables forwarding of IPv6 unicast datagrams.	GC

Command	Description	Mode^a
ping ipv6	Determines whether another computer is on the network.	PE
ping ipv6 interface	Determines whether another computer is on the network using Interface keyword.	PE
show ipv6 brief	Displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.	PE
show ipv6 interface	Shows the usability status of IPv6 interfaces.	PE
show ipv6 mld groups	Displays information about multicast groups that MLD reported.	PE
show ipv6 mld interface	Displays MLD related information for an interface.	PE
show ipv6 mld-proxy	Displays a summary of the host interface status parameters.	PE
show ipv6 mld-proxy groups	Displays information about multicast groups that the MLD Proxy reported.	PE
show ipv6 mld-proxy groups detail	Displays information about multicast groups that MLD Proxy reported.	PE
show ipv6 mld-proxy interface	Displays a detailed list of the host interface status parameters.	PE
show ipv6 mld traffic	Displays MLD statistical information for the router.	PE
show ipv6 neighbors	Displays information about IPv6 neighbors.	PE
show ipv6 route	Displays the IPv6 routing table.	PE
show ipv6 route preferences	Shows the preference value associated with the type of route.	PE
show ipv6 route summary	Displays a summary of the routing table.	PE
show ipv6 traffic	Shows traffic and statistics for IPv6 and ICMPv6.	UE
show ipv6 vlan	Displays IPv6 VLAN routing interface addresses.	PE

Command	Description	Mode ^a
<code>traceroute ipv6</code>	Discovers the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Loopback Interface

Command	Description	Mode ^a
<code>interface loopback</code>	Enters the Interface Loopback configuration mode.	GC
<code>show interfaces loopback</code>	Displays information about configured loopback interfaces.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Multicast

Command	Description	Mode ^a
<code>ip mcast boundary</code>	Adds an administrative scope multicast boundary.	IC
<code>ip mroute</code>	Creates a static multicast route for a source range.	GC
<code>ip multicast</code>	Sets the administrative mode of the IP multicast forwarder in the router to active.	GC
<code>ip multicast ttl-threshold</code>	Applies a <i>ttlvalue</i> to a routing interface.	IC
<code>ip pim</code>	Administratively configures PIM mode for IP multicast routing on a VLAN interface.	IC
<code>ip pim bsr-border</code>	Administratively disables bootstrap router (BSR) messages from being sent or received through an interface.	IC
<code>ip pim bsr-candidate</code>	Configures the router to advertise itself as a bootstrap router (BSR).	GC
<code>ip pim dense</code>	Administratively configures PIM dense mode for IP multicast routing.	GC

Command	Description	Mode^a
<code>ip pim dr-priority</code>	Administratively configures the advertised designated router (DR) priority value.	IC
<code>ip pim hello-interval</code>	Administratively configures the PIM Hello messages on the specified interface.	IC
<code>ip pim join-prune-interval</code>	Administratively configures the frequency of join/prune messages on the specified interface.	IC
<code>ip pim register-rate-limit</code>	Sets a limit on the maximum number of PIM register messages sent per second for each (S,G) entry.	GC
<code>ip pim rp-address</code>	Defines the address of a PIM RP for a specific multicast group range.	GC
<code>ip pim rp-candidate</code>	Configures the router to advertise itself to the bootstrap router (BSR) as a PIM candidate rendezvous point (RP) for a specific multicast group range.	IC
<code>ip pim sparse</code>	Administratively configures PIM sparse mode for IP multicast routing.	GC
<code>ip pim ssm</code>	Administratively configures PIM Source Specific Multicast (SSM) range of addresses for IP multicast routing.	GC
<code>ip pim spt-threshold</code>	Sets the multicast traffic threshold rate for the last-hop router to switch to the shortest path on the router.	GC
<code>show ip multicast</code>	Displays the system-wide multicast information.	PE
<code>show ip mcast boundary</code>	Displays the system-wide multicast information.	PE
<code>show ip multicast interface</code>	Displays the multicast information for the specified interface.	PE
<code>show ip mcast mroute</code>	Displays a summary or all the details of the multicast table.	PE
<code>show ip mcast mroute group</code>	Displays the multicast configuration settings of entries in the multicast mroute table.	PE

Command	Description	Mode^a
<code>show ip mcast mroute source</code>	Displays the multicast configuration settings of entries in the multicast mroute table.	PE
<code>show ip mcast mroute static</code>	Displays all the static routes configured in the static mcast table.	PE
<code>show ip pim bsr-router</code>	Displays the bootstrap router (BSR) information.	PE
<code>show ip pim interface</code>	Displays PIM interface status parameters. If no interface is specified, the command displays the status parameters of all PIM-enabled interfaces.	UE or PE
<code>show ip pim neighbor</code>	Displays PIM neighbors discovered by PIMv2 Hello messages. If no interface is specified, the command displays the neighbors discovered on all PIM-enabled interfaces.	UE or PE
<code>show ip pim rp hash</code>	Displays the rendezvous point (RP) selected for the specified group address.	UE or PE
<code>show ip pim rp mapping</code>	Displays the mappings for the PIM group to the active rendezvous points (RPs).	UE or PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

IPv6 Multicast

Command	Description	Mode^a
<code>ipv6 pim (Global config)</code>	Administratively enables PIMSM for IPv6 multicast routing	GC
<code>ipv6 pim (VLAN Interface config)</code>	Administratively enables PIM-SM multicast routing mode on a particular IPv6 router interface.	IC
<code>ipv6 pim bsr-border</code>	Prevents bootstrap router (BSR) messages from being sent or received through an interface.	IC
<code>ipv6 pim bsr-candidate</code>	Configures the router to announce its candidacy as a bootstrap router (BSR).	GC
<code>ipv6 pim dense</code>	Administratively configures PIM dense mode for IPv6 multicast routing.	GC

Command	Description	Mode^a
<code>ipv6 pim dr-priority</code>	Sets the priority value for which a router is elected as the designated router (DR).	IC
<code>ipv6 pim hello-interval</code>	Administratively configures the PIM-SM Hello Interval for the specified interface.	IC
<code>ipv6 pim join-prune-interval</code>	Administratively configures the interface join/prune interval for the PIM-SM router.	IC
<code>ipv6 pim register-rate-limit</code>	Sets a limit on the maximum number of PIM register messages sent per second for each (S,G) entry	GC
<code>ipv6 pim register-threshold</code>	Configures the Register Threshold rate for the RP router to switch to the shortest path.	GC
<code>ipv6 pim rp-address</code>	Statically configures the Rendezvous Point (RP) address for one or more multicast groups.	GC
<code>ipv6 pim rp-candidate</code>	Configures the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).	GC
<code>ipv6 pim sparse (Global config)</code>	Administratively configures PIM sparse mode for multicast routing.	GC
<code>ipv6 pim spt-threshold</code>	Configures the Data Threshold rate for the last-hop router to switch to the shortest path.	GC
<code>ipv6 pim ssm</code>	Defines the Source Specific Multicast (SSM) range of multicast addresses.	GC
<code>show ipv6 pim</code>	Displays global status of IPv6 PIMSM and its IPv6 routing interfaces.	PE or GC
<code>show ipv6 pim bsr</code>	Displays the bootstrap router (BSR) information.	PE or GC
<code>show ipv6 pim bsr-router</code>	Display the bootstrap router (BSR) information.	UE, PE, or GC
<code>show ipv6 pim interface</code>	Displays interface config parameters.	PE or GC

Command	Description	Mode ^a
<code>show ipv6 pim neighbor</code>	Displays IPv6 PIMSM neighbors learned on the routing interfaces.	PE or GC
<code>show ipv6 pim rphash</code>	Displays which rendezvous point (RP) is being selected for a specified group.	PE or GC
<code>show ipv6 pim rp mapping</code>	Displays all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)).	PE or GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

OSPF

Command	Description	Mode ^a
<code>area default-cost (Router OSPF)</code>	Configures the advertised default cost for the stub area.	ROSPF
<code>area nssa (Router OSPF)</code>	Configures the specified area ID to function as an NSSA.	ROSPF
<code>area nssa default-info-originate (Router OSPF Config)</code>	Configures the metric value and type for the default route advertised into the NSSA.	ROSPF
<code>area nssa no-redistribute</code>	Configures the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.	ROSPF
<code>area nssa no-summary</code>	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSPF
<code>area nssa translator-role</code>	Configures the translator role of the NSSA.	ROSPF
<code>area nssa translator-stab-intv</code>	Configures the translator stability interval of the NSSA.	ROSPF
<code>area range (Router OSPF)</code>	Creates a specified area range for a specified NSSA.	ROSPF
<code>area stub</code>	Creates a stub area for the specified area ID.	ROSPF
<code>area stub no-summary</code>	Prevents Summary LSAs from being advertised into the NSSA.	ROSPF

Command	Description	Mode^a
<code>area virtual-link</code>	Creates the OSPF virtual interface for the specified area-id and neighbor router.	ROSPF
<code>area virtual-link authentication</code>	Configures the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID.	ROSPF
<code>area virtual-link dead-interval</code>	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router.	ROSPF
<code>area virtual-link hello-interval</code>	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
<code>area virtual-link retransmit-interval</code>	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
<code>area virtual-link transmit-delay</code>	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
<code>auto-cost</code>	Allows user to change the reference bandwidth used in computing link cost.	ROSPF
<code>bandwidth</code>	Allows user to change the bandwidth used in computing link cost.	IC
<code>capability opaque</code>	Enables Opaque Capability on the router.	RC
<code>clear ip ospf</code>	Resets specific OSPF states.	PE
<code>compatible rfc1583</code>	Enables OSPF 1583 compatibility.	ROSPF
<code>default-information originate (Router OSPF Configuration)</code>	Controls the advertisement of default routes.	ROSPF
<code>default-metric</code>	Sets a default for the metric of distributed routes.	ROSPF
<code>distance ospf</code>	Sets the route preference value of OSPF in the router.	ROSPF
<code>distribute-list out</code>	Specifies the access list to filter routes received from the source protocol.	ROSPF

Command	Description	Mode^a
enable	Resets the default administrative mode of OSPF in the router (active).	ROSPF
exit-overflow-interval	Configures the exit overflow interval for OSPF.	ROSPF
external-lsdb-limit	Configures the external LSDB limit for OSPF.	ROSPF
ip ospf area	Enables OSPFv2 and sets the area ID of an interface.	IC
ip ospf authentication	Sets the OSPF Authentication Type and Key for the specified interface.	IC
ip ospf cost	Configures the cost on an OSPF interface.	IC
ip ospf dead-intervall	Sets the OSPF dead interval for the specified interface.	IC
ip ospf hello-interval	Sets the OSPF hello interval for the specified interface.	IC
ip ospf mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
ip ospf network	Configure OSPF to treat an interface as a point-to-point, rather than broadcast interface.	IC
ip ospf priority	Sets the OSPF priority for the specified router interface.	IC
ip ospf retransmit-interval	Sets the OSPF retransmit Interval for the specified interface.	IC
ip ospf transmit-delay	Sets the OSPF Transit Delay for the specified interface.	IC
maximum-paths	Sets the number of paths that OSPF can report for a given destination.	ROSPF
nsf helper	Allow OSPF to act as a helpful neighbor for a restarting router.	ROSPF
nsf helper strict-lsa-checking	Set an OSPF helpful neighbor exit helper mode whenever a topology change occurs.	ROSPF
nsf restart-interval	Configures the length of the grace period on the restarting router.	ROSPF

Command	Description	Mode^a
network area	Enables OSPFv2 on an interface and sets its area ID if the IP address of an interface is covered by this network command.	ROSPF
passive-interface	Sets the interface or tunnel as passive.	IC
passive-interface default	Enables the global passive mode by default for all interfaces.	ROSPF
passive-interface	Sets the interface or tunnel as passive.	ROSPF
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	ROSPF
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.	ROSPF
router ospf	Enters Router OSPF mode.	CC
show ip ospf	Displays information relevant to the OSPF router.	PE
show ip ospf abr	Displays the internal OSPF routing table entries to Area Border Routers (ABR).	PE
show ip ospf area	Displays information about the identified OSPF area.	PE
show ip ospf asbr	Displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR).	PE
show ip ospf database	Displays information about the link state database when OSPF is enabled.	PE
show ip ospf database database-summary	Displays the number of each type of LSA in the database for each area and for the router.	PE
show ip ospf interface	Displays the information for the IFO object or virtual interface tables.	PE
show ip ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ip ospf interface stats	Displays the statistics for a specific interface.	PE
show ip ospf neighbor	Displays information about OSPF neighbors.	PE

Command	Description	Mode^a
<code>show ip ospf range</code>	Displays information about the area ranges for the specified area-id.	PE
<code>show ip ospf statistics</code>	Displays information about recent Shortest Path First (SPF) calculations.	PE
<code>show ip ospf stub table</code>	Displays the OSPF stub table.	PE
<code>show ip ospf virtual-link</code>	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
<code>show ip ospf virtual-links brief</code>	Displays the OSPF Virtual Interface information for all areas in the system.	PE
<code>show routing heap summary</code>	Displays a summary of the memory allocation from the routing heap.	PE
<code>timers pacing flood</code>	Adjusts the rate at which OSPFv2 sends LS Update packets	OG
<code>timers pacing lsa-group</code>	Tunes how OSPF groups LSAs for periodic refresh.	OG
<code>timers spf</code>	Configures the SPF delay and hold time.	ROSPF

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

OSPFv3

Command	Description	Mode^a
<code>area default-cost (Router OSPFv3)</code>	Configures the monetary default cost for the stub area.	ROSV3
<code>area nssa (Router OSPFv3)</code>	Configures the specified areaid to function as an NSSA.	ROSV3
<code>area nssa default-info-originate (Router OSPFv3 Config)</code>	Configures the metric value and type for the default route advertised into the NSSA.	ROSV3
<code>area nssa no-redistribute</code>	Configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.	ROSV3
<code>area nssa no-summary</code>	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSV3

Command	Description	Mode^a
<code>area nssa translator-role</code>	Configures the translator role of the NSSA.	ROSV3
<code>area nssa translator-stab-intv</code>	Configures the translator stability interval of the NSSA.	ROSV3
<code>area range (Router OSPFv3)</code>	Creates an area range for a specified NSSA.	ROSV3
<code>area stub</code>	Creates a stub area for the specified area ID.	ROSV3
<code>area stub no-summary</code>	Disables the import of Summary LSAs for the stub area identified by <i>areaid</i> .	ROSV3
<code>area virtual-link</code>	Creates the OSPF virtual interface for the specified <i>areaid</i> and <i>neighbor</i> .	ROSV3
<code>area virtual-link dead-interval</code>	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
<code>area virtual-link hello-interval</code>	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
<code>area virtual-link retransmit-interval</code>	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
<code>area virtual-link transmit-delay</code>	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
<code>default-information originate (Router OSPFv3 Configuration)</code>	Controls the advertisement of default routes.	ROSV3
<code>default-metric</code>	Sets a default for the metric of distributed routes.	ROSV3
<code>distance ospf</code>	Sets the route preference value of OSPF in the router.	ROSV3
<code>enable</code>	Resets the default administrative mode of OSPF in the router (active).	ROSV3
<code>exit-overflow-interval</code>	Configures the exit overflow interval for OSPF.	ROSV3
<code>external-lsdb-limit</code>	Configures the external LSDB limit for OSPF.	ROSV3

Command	Description	Mode^a
<code>ipv6 ospf</code>	Enables OSPF on a router interface or loopback interface.	IC
<code>ipv6 ospf area</code>	Sets the OSPF area to which the specified router interface belongs.	IC
<code>ipv6 ospf cost</code>	Configures the cost on an OSPF interface.	IC
<code>ipv6 ospf dead-interval</code>	Sets the OSPF dead interval for the specified interface.	IC
<code>ipv6 ospf hello-interval</code>	Sets the OSPF hello interval for the specified interface.	IC
<code>ipv6 ospf mtu-ignore</code>	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
<code>ipv6 ospf network</code>	Changes the default OSPF network type for the interface.	IC
<code>ipv6 ospf priority</code>	Sets the OSPF priority for the specified router interface.	IC
<code>ipv6 ospf retransmit-interval</code>	Sets the OSPF retransmit interval for the specified interface.	IC
<code>ipv6 ospf transmit-delay</code>	Sets the OSPF Transmit Delay for the specified interface.	IC
<code>ipv6 router ospf</code>	Enters Router OSPFv3 Configuration mode.	GC
<code>maximum-paths</code>	Sets the number of paths that OSPF can report for a given destination.	ROSV3
<code>nsf</code>	Enables OSPF graceful restart.	ROSV3
<code>nsf helper</code>	Allows OSPF to act as a helpful neighbor for a restarting router.	ROSV3
<code>nsf helper strict-lsa-checking</code>	Requires that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.	ROSV3
<code>nsf restart-interval</code>	Configures the length of the grace period on the restarting router.	ROSV3
<code>passive-interface</code>	Sets the interface or tunnel as passive.	IC
<code>passive-interface default</code>	Enables the global passive mode by default for all interfaces.	ROSV3

Command	Description	Mode^a
redistribute	Configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.	ROSV3
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.	ROSV3
show ipv6 ospf	Displays information relevant to the OSPF router.	PE
show ipv6 ospf abr	Displays the internal OSPFv3 routes to reach Area Border Routers (ABR).	PE
show ipv6 ospf area	Displays information about the area.	PE
show ipv6 ospf asbr	Displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR).	PE
show ipv6 ospf border-routers	Displays internal OSPFv3 routers to reach Area Border Routers (ABR) and Autonomous System Boundary Routes (ASBR).	UE or PE
show ipv6 ospf database	Displays information about the link state database when OSPFv3 is enabled.	PE
show ipv6 ospf database database-summary	Displays the number of each type of LSA in the database and the total number of LSAs in the database.	PE
show ipv6 ospf interface	Displays the information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface stats	Displays the statistics for a specific interface.	UE
show ipv6 ospf interface vlan	Displays OSPFv3 configuration and status information for a specific VLAN.	PE
show ipv6 ospf neighbor	Displays information about OSPF neighbors.	PE
show ipv6 ospf range	Displays information about the area ranges for the specified area identifier.	PE
show ipv6 ospf stub table	Displays the OSPF stub table.	PE

Command	Description	Mode ^a
<code>show ipv6 ospf virtual-links</code>	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
<code>show ipv6 ospf virtual-link brief</code>	Displays the OSPFV3 Virtual Interface information for all areas in the system.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Router Discovery Protocol

Command	Description	Mode ^a
<code>ip irdp</code>	Enables Router Discovery on an interface.	IC
<code>ip irdp address</code>	Configures the address that the interface uses to send the router discovery advertisements.	IC
<code>ip irdp holdtime</code>	Configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.	IC
<code>ip irdp maxadvertinterval</code>	Configures the maximum time, in seconds, allowed between sending router advertisements from the interface.	IC
<code>ip irdp minadvertinterval</code>	Configures the minimum time, in seconds, allowed between sending router advertisements from the interface.	IC
<code>ip irdp multicast</code>	Sends router advertisements as IP multicast packets.	IC
<code>ip irdp preference</code>	Configures the preference of the address as a default router address relative to other router addresses on the same subnet.	IC
<code>show ip irdp</code>	Displays the router discovery information for all interfaces, or for a specified interface.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Routing Information Protocol

Command	Description	Mode ^a
<code>auto-summary</code>	Enables the RIP auto-summarization mode.	RIP

Command	Description	Mode^a
default-information originate (Router RIP Configuration)	Controls the advertisement of default routes.	RIP
default-metric	Sets a default for the metric of distributed routes.	RIP
distance rip	Sets the route preference value of RIP in the router.	RIP
distribute-list out	Specifies the access list to filter routes received from the source protocol.	RIP
enable	Resets the default administrative mode of RIP in the router (active).	RIP
hostroutesaccept	Enables the RIP hostroutesaccept mode.	RIP
ip rip	Enables RIP on a router interface.	IC
ip rip authentication	Sets the RIP Version 2 Authentication Type and Key for the specified interface.	IC
ip rip receive version	Configures the interface to allow RIP control packets of the specified version(s) to be received.	IC
ip rip send version	Configures the interface to allow RIP control packets of the specified version to be sent.	IC
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	PIP
router rip	Enters Router RIP mode.	GC
show ip rip	Displays information relevant to the RIP router.	PE
show ip rip interface	Displays information related to a particular RIP interface.	PE
show ip rip interface brief	Displays general information for each RIP interface.	PE
split-horizon	Sets the RIP split horizon mode.	RIP

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Tunnel Interface

Command	Description	Mode ^a
<code>interface tunnel</code>	Enables the interface configuration mode for a tunnel.	GC
<code>show interfaces tunnel</code>	Displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.	PE
<code>tunnel destination</code>	Specifies the destination transport address of the tunnel.	IC
<code>tunnel mode ipv6ip</code>	Specifies the mode of the tunnel.	IC
<code>tunnel source</code>	Specifies the source transport address of the tunnel, either explicitly or by reference to an interface.	IC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Virtual Router Redundancy

Command	Description	Mode ^a
<code>ip vrrp</code>	Enables the administrative mode of Virtual Router Redundancy Protocol (VRRP) for the router.	GC
<code>vrrp accept-mode</code>	Enables the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.	IC
<code>vrrp authentication</code>	Sets the authentication details value for the virtual router configured on a specified interface.	IC
<code>vrrp description</code>	Assigns a description to the VRRP group.	IC
<code>vrrp ip</code>	Sets the virtual router IP address value for an interface.	IC
<code>vrrp mode</code>	Enables the virtual router configured on an interface. Enabling the status field starts a virtual router.	IC

Command	Description	Mode^a
<code>vrrp preempt</code>	Sets the preemption mode value for the virtual router configured on a specified interface.	IC
<code>vrrp priority</code>	Sets the priority value for the virtual router configured on a specified interface.	IC
<code>vrrp timers advertise</code>	Sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.	IC
<code>vrrp timers learn</code>	Configures the router, when it is acting as backup virtual router for a VRRR group, to learn the advertisement interval used by the master virtual router.	IC
<code>vrrp track interface</code>	Alters the priority of the VRRP router based on the availability of its interfaces.	IC
<code>vrrp track ip route</code>	Tracks route reachability.	IC
<code>show vrrp</code>	Displays the global VRRP configuration and status as well as the brief or detailed status of one or all VRRP groups.	UE or PE
<code>show vrrp interface</code>	Displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.	UE or PE
<code>show vrrp interface brief</code>	Displays information about each virtual router configured on the switch.	PE
<code>show vrrp interface stats</code>	Displays the statistical information about each virtual router configured on the switch.	PE
Pingable VRRP Commands		
<code>ip vrrp accept-mode</code>	Enables the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.	IC
<code>show ip vrrp interface</code>	Displays the configured value for Accept Mode.	UE or PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Utility Commands

Auto-Install

Command	Description	Mode ^a
<code>boot auto-copy-sw</code>	Enables or disables Stack Firmware Synchronization.	GC
<code>boot auto-copy-sw allow-downgrade</code>	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.	GC
<code>boot host autoreboot</code>	Enables rebooting the device (no administrative intervention) when the auto-image is successfully downloaded.	GC
<code>boot host autosave</code>	Enables/disables automatically saving the downloaded configuration on the switch.	GC
<code>boot host dhcp</code>	Enables/disables Auto Config on the switch.	GC
<code>boot host retrycount</code>	Set the number of attempts to download a configuration.	GC
<code>show auto-copy-sw</code>	Displays Stack Firmware Synchronization configuration status.	PE
<code>show boot</code>	Displays the current status of the Auto Config process.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Captive Portal

Command	Description	Mode ^a
<code>authentication timeout</code>	Configures the authentication timeout.	CP
<code>captive-portal</code>	Enables the captive portal configuration mode.	GC
<code>enable</code>	Globally enables captive portal.	CPI
<code>http port</code>	Configures an additional HTTP port for captive portal to monitor.	CP

Command	Description	Mode^a
https port	Configures an additional HTTPS port for captive portal to monitor.	CP
show captive-portal	Displays the status of captive portal.	PE
show captive-portal status	Reports the status of all captive portal instances in the system.	PE
block	Blocks all traffic for a captive portal configuration.	CPI
configuration	Enables the captive portal instance mode.	CP
enable	Enables a captive portal configuration.	CPI
group	Configures the group number for a captive portal configuration.	CPI
interface	Associates an interface with a captive portal configuration.	CPI
locale	Associates an interface with a captive portal configuration.	CPI
name (Captive Portal)	Configures the name for a captive portal configuration.	CPI
protocol	Configures the protocol mode for a captive portal configuration.	CPI
redirect	Enables the redirect mode for a captive portal configuration.	CPI
redirect-url	Configures the redirect URL for a captive portal configuration.	CPI
session-timeout	Configures the session timeout for a captive portal configuration.	CPI
verification	Configures the verification mode for a captive portal configuration.	CPI
captive-portal client deauthenticate	Deauthenticates a specific captive portal client.	PE
show captive-portal client status	Displays client connection details or a connection summary for connected captive portal users.	PE

Command	Description	Mode^a
<code>show captive-portal configuration client status</code>	Displays the clients authenticated to all captive portal configurations or a to specific configuration.	PE
<code>show captive-portal interface client status</code>	Displays information about clients authenticated on all interfaces or a specific interface.	PE
<code>show captive-portal interface configuration status</code>	Displays the clients authenticated to all captive portal configurations or a to specific configuration.	PE
<code>clear captive-portal users</code>	Deletes all captive portal user entries.	PE
<code>no user</code>	Deletes a user from the local user database.	CP
<code>show captive-portal user</code>	Displays all configured users or a specific user in the captive portal local user database.	PE
<code>user group</code>	Associates a group with a captive portal user.	
<code>user-logout</code>	Enables captive portal users to log out of the portal.	CPI
<code>user name</code>	Modifies the user name for a local captive portal user.	CP
<code>user password</code>	Creates a local user or changes the password for an existing user.	CP
<code>user session-timeout</code>	Sets the session timeout value for a captive portal user.	CP
<code>show captive-portal configuration</code>	Displays the operational status of each captive portal configuration.	PE
<code>show captive-portal configuration interface</code>	Displays information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration.	PE
<code>show captive-portal configuration locales</code>	Displays locales associated with a specific captive portal configuration.	PE
<code>show captive-portal configuration status</code>	Displays information about all configured captive portal configurations or a specific captive portal configuration.	PE

Command	Description	Mode ^a
user group	Creates a user group.	CP
user group moveusers	Moves a group's users to a different group.	CP
user group name	Configures a group name.	CP

- a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

CLI Macro

Command	Description	Mode ^a
macro name	Creates a user-defined macro.	GC
macro global apply	Use to apply a macro.	GC
macro global trace	Applies and traces a macro.	GC
macro global description	Appends a line to the global macro description.	GC
macro apply	Use to apply a macro.	IC
macro trace	Applies and traces a macro.	IC
macro description	Appends a line to the macro description.	IC
show parser macro	Displays information about defined macros.	PE

- a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Clock

Command	Description	Mode ^a
show sntp configuration	Displays the SNTP configuration.	PE
show sntp server	Displays the pre-configured SNTP servers.	PE
show sntp status	Displays the SNTP status.	PE
sntp authenticate	Set to require authentication for received NTP traffic from servers.	GC
sntp authentication-key	Defines an authentication key for SNTP.	GC
sntp broadcast client enable	Enables SNTP Broadcast clients.	GC
sntp client poll timer	Defines polling time for the SNTP client.	GC

Command	Description	Mode ^a
ntp server	Configures the SNTP server to use SNTP to request and accept NTP traffic from it.	GC
ntp trusted-key	Authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize.	GC
ntp unicast client enable	Enables clients to use Simple Network Time Protocol (SNTP) predefined Unicast clients.	GC
clock timezone hours-offset	Sets the offset to Coordinated Universal Time.	GC
clock summer-time recurring	Sets the summertime offset to UTC recursively every year.	GC
clock summer-time date	Sets the summertime offset to UTC.	GC
show clock	Displays the time and date from the system clock.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Command Line Configuration Scripting

Command	Description	Mode ^a
script apply	Applies commands in the script to the switch.	PE
script delete	Deletes a specific script.	PE
script list	Lists all scripts present in the switch.	PE
script show	Displays the contents of a script file.	PE
script validate	Validates a script file.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Configuration and Image Files

Command	Description	Mode ^a
boot system	Specifies the system image that the switch loads at startup.	PE
clear config	Restores switch to default configuration.	PE
copy	Copies files from a source to a destination.	PE

Command	Description	Mode^a
delete	Deletes a file from a flash memory.	PE
delete backup-image	Deletes a file from a flash memory device.	PE
delete backup-config	Deletes the backup configuration file.	PE
delete startup-config	Deletes the startup configuration file.	PE
dir	Prints the contents of the flash file system.	PE
erase	Erases the startup configuration, the backup configuration, or the backup image.	PE
filedescr	Adds a description to a file.	PE
rename	Renames the file present in flash.	PE
show backup-config	Displays contents of a backup configuration file.	PE
show bootvar	Displays the active system image file that the switch loads at startup.	UE
show running-config	Displays the contents of the currently running configuration file.	PE
show startup-config	Displays the startup configuration file contents.	PE
update bootcode	Updates the bootcode on one or more switches.	PE
write	Copies the running configuration image to the startup configuration.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Denial of Service

Command	Description	Mode^a
dos-control firstfrag	Enables Minimum TCP Header Size Denial of Service protection.	GC
dos-control icmp	Enables Maximum ICMP Packet Size Denial of Service protections.	GC
dos-control l4port	Enables L4 Port Denial of Service protection.	GC
dos-control sipdip	Enables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection.	GC

Command	Description	Mode^a
dos-control tcpflag	Enables TCP Flag Denial of Service protections.	GC
dos-control tcpfrag	Enables TCP Fragment Denial of Service protection.	GC
ip icmp echo-reply	Enables or disables the generation of ICMP Echo Reply messages.	GC
ip icmp error-interval	Limits the rate at which IPv4 ICMP error messages are sent.	GC
ip unreachable	Enables the generation of ICMP Destination Unreachable messages.	IC
ip redirects	Enables the generation of ICMP Redirect messages.	IC
ipv6 icmp error-interval	Limits the rate at which ICMPv6 error messages are sent.	GC
ipv6 unreachable	Enables the generation of ICMPv6 Destination Unreachable messages.	IC
show dos-control	Displays Denial of Service configuration information.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Line

Command	Description	Mode^a
exec-timeout	Configures the interval that the system waits for user input.	LC
history	Enables the command history function.	LC
history size	Changes the command history buffer size for a particular line.	LC
line	Identifies a specific line for configuration and enters the line configuration command mode.	GC
show line	Displays line parameters.	UE
speed	Sets the line baud rate.	LC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Management ACL

Command	Description	Mode ^a
deny (management)	Defines a deny rule.	MA
management access-class	Defines which management access-list is used.	GC
management access-list	Defines a management access-list, and enters the access-list for configuration.	GC
permit (management)	Defines a permit rule.	MA
show management access-class	Displays the active management access-list.	PE
show management access-list	Displays management access-lists.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Mode

Command	Description	Mode ^a
configure terminal	Gets to the configure line. This command is equivalent to the configure command.	PE
do	Executes commands available in Privileged EXEC mode from Global Configuration and other modes.	All except PE and UE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Password Management

Command	Description	Mode ^a
passwords aging	Implements aging on the passwords such that users are required to change passwords when they expire.	GC
passwords history	Enables the administrator to set the number of previous passwords that are stored to ensure that users do not reuse their passwords too frequently.	GC

Command	Description	Mode^a
<code>passwords lock-out</code>	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.	GC
<code>passwords min-length</code>	Enables the administrator to enforce a minimum length required for a password.	GC
<code>passwords strength-check</code>	Enables the Password Strength feature.	GC
<code>passwords strength minimum uppercase-letters</code>	Enforces a minimum number of uppercase letters that a password should contain.	GC
<code>passwords strength minimum lowercase-letters</code>	Enforces a minimum number of lowercase letters that a password must contain.	GC
<code>passwords strength minimum numeric-characters</code>	Enforces a minimum number of numeric numbers that a password should contain.	GC
<code>passwords strength minimum special-characters</code>	Enforces a minimum number of special characters that a password may contain.	GC
<code>passwords strength max-limit consecutive-characters</code>	Enforces a maximum number of consecutive characters that a password can contain.	GC
<code>passwords strength max-limit repeated-characters</code>	Enforces a maximum repeated characters that a password should contain.	GC
<code>passwords strength minimum character-classes</code>	Enforces the minimum number of character classes (uppercase letters, lowercase letters, numeric characters and special characters) that a password must contain.	GC
<code>passwords strength exclude-keyword</code>	Enforces a maximum number of consecutive characters that a password can contain.	GC
<code>enable password encrypted</code>	Used by an Administrator to transfer the enable password between devices without having to know the password.	PE
<code>show passwords configuration</code>	Displays the configuration parameters for password configuration.	PE
<code>show passwords result</code>	Displays the last password set result information.	PE

- a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

PHY Diagnostics

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

- a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

RMON

Command	Description	Mode ^a
rmon alarm	Configures alarm conditions.	GC
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	IC
rmon event	Configures an RMON event.	GC
show rmon alarm	Displays alarm configurations.	UE
show rmon alarms	Displays the alarms summary table.	UE and PE
show rmon collection history	Displays the requested group of statistics.	UE
show rmon events	Displays the RMON event table.	UE
show rmon history	Displays RMON Ethernet Statistics history.	UE
show rmon log	Displays the RMON logging table.	UE
show rmon statistics	Displays RMON Ethernet Statistics.	UE

- a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

SDM Templates

Command	Description	Mode ^a
<code>sdm prefer</code>	Changes the template that will be active after the next reboot.	GC
<code>show sdm prefer</code>	Views the currently active SDM template and its scaling parameters, or views the scaling parameters for an inactive template.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Serviceability Tracing

Command	Description	Mode ^a
<code>debug arp</code>	Enables tracing of ARP packets.	PE
<code>debug auto-voip</code>	Enables Auto VOIP debug messages.	PE
<code>debug clear</code>	Disables all debug traces.	PE
<code>debug console</code>	Enables the display of debug trace output on the login session in which it is executed.	PE
<code>debug dot1x</code>	Enables dot1x packet tracing.	PE
<code>debug igmpsnooping</code>	Enables tracing of IGMP Snooping packets transmitted and/or received by the switch.	PE
<code>debug ip acl</code>	Enables debug of IP Protocol packets matching the ACL criteria.	PE
<code>debug ip dvmrp</code>	Traces DVMRP packet reception and transmission.	PE
<code>debug ip igmp</code>	Traces IGMP packet reception and transmission.	PE
<code>debug ip mcache</code>	Traces MDATA packet reception and transmission.	PE
<code>debug ip pimdm packet</code>	Traces PIMDM packet reception and transmission.	PE
<code>debug ip pimsm packet</code>	Traces PIMSM packet reception and transmission.	PE
<code>debug ip vrrp</code>	Enables VRRP debug protocol messages.	PE

Command	Description	Mode^a
<code>debug ipv6 dhcp</code>	Displays debug information about DHCPv6 client activities and to trace DHCPv6 packets to and from the local DHCPv6 client.	PE
<code>debug ipv6 mcache</code>	Traces MDATAv6 packet reception and transmission.	PE
<code>debug ipv6 mld</code>	Traces MLD packet reception and transmission.	PE
<code>debug ipv6 pimdm</code>	Traces PIMDMv6 packet reception and transmission.	PE
<code>debug ipv6 pimsm</code>	Traces PIMSMv6 packet reception and transmission.	PE
<code>debug isdp</code>	Traces ISDP packet reception and transmission.	PE
<code>debug lacp</code>	Traces of LACP packets received and transmitted by the switch.	PE
<code>debug mldsnopping</code>	Traces MLD snooping packet reception and transmission.	PE
<code>debug ospf</code>	Enables tracing of OSPF packets received and transmitted by the switch.	PE
<code>debug ospfv3</code>	Enables tracing of OSPFv3 packets received and transmitted by the switch.	PE
<code>debug ping</code>	Enables tracing of ICMP echo requests and responses.	PE
<code>debug rip</code>	Enables tracing of RIP requests and responses.	PE
<code>debug sflow</code>	Enables sFlow debug packet trace.	PE
<code>debug spanning-tree</code>	Traces spanning tree BPDU packet reception and transmission.	PE
<code>debug vrrp</code>	Enables VRRP debug protocol messages.	PE
<code>show debugging</code>	Displays packet tracing configurations.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

sFlow

Command	Description	Mode ^a
sflow destination	Configures sFlow collector parameters (owner string, receiver timeout, ip address, and port).	GC
sflow polling	Enables a new sflow poller instance for the data source if rcvr_idx is valid.	GC
sflow polling (Interface Mode)	Enable a new sflow poller instance for this data source if rcvr_idx is valid.	IC
sflow sampling	Enables a new sflow sampler instance for this data source if rcvr_idx is valid.	GC
sflow sampling (Interface Mode)	Enables a new sflow sampler instance for this data source if rcvr_idx is valid.	IC
show sflow agent	Displays the sflow agent information.	PE
show sflow destination	Displays all the configuration information related to the sFlow receivers.	PE
show sflow polling	Displays the sFlow polling instances created on the switch.	PE
show sflow sampling	Displays the sFlow sampling instances created on the switch.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

SNMP

Command	Description	Mode ^a
show snmp	Displays the SNMP status.	PE
show snmp engineID	Displays the SNMP engine ID.	PE
show snmp filters	Displays the configuration of filters.	PE
show snmp group	Displays the configuration of groups.	PE
show snmp user	Displays the configuration of users.	PE
show snmp views	Displays the configuration of views.	PE
show trapflags	Displays SNMP traps globally or displays specific SNMP traps.	PE

Command	Description	Mode^a
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	GC
snmp-server community-group	Maps SNMP v1 and v2 security models to the group name.	GC
snmp-server contact	Sets up a system contact (sysContact) string.	GC
snmp-server enable traps	Enables SNMP traps globally or enables specific SNMP traps.	GC
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engine ID on the local switch.	GC
snmp-server filter	Creates or updates an SNMP server filter entry.	GC
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	GC
snmp-server host	Specifies the recipient of SNMP notifications.	GC
snmp-server location	Sets the system location string.	GC
snmp-server user	Configures a new SNMP Version 3 user.	GC
snmp-server view	Creates or updates a Simple Network Management Protocol (SNMP) server view entry.	GC
snmp-server v3-host	Specifies the recipient of Simple Network Management Protocol Version 3 (SNMPv3) notifications.	GC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

SSH

Command	Description	Mode^a
crypto key generate dsa	Generates DSA key pairs for the switch.	GC
crypto key generate rsa	Generates RSA key pairs for the switch.	GC
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.	GC
ip ssh port	Specifies the port to be used by the SSH server.	GC

Command	Description	Mode ^a
<code>ip ssh pubkey-auth</code>	Enables public key authentication for incoming SSH sessions.	GC
<code>ip ssh server</code>	Enables the switch to be configured from a SSH server connection.	GC
<code>key-string</code>	Manually specifies a SSH public key.	SK
<code>show crypto key mypubkey</code>	Displays its own SSH public keys stored on the switch.	PE
<code>show crypto key pubkey-chain ssh</code>	Displays SSH public keys stored on the switch.	PE
<code>show ip ssh</code>	Displays the SSH server configuration.	PE
<code>user-key</code>	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SP

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Syslog

Command	Description	Mode ^a
<code>clear logging</code>	Clears messages from the internal logging buffer.	PE
<code>clear logging file</code>	Clears messages from the logging file.	PE
<code>description (Logging)</code>	Describes the syslog server.	L
<code>level</code>	Specifies the importance level of syslog messages.	L
<code>logging cli-command</code>	Enable CLI command logging.	GC
<code>logging</code>	Logs messages to a syslog server.	GC
<code>logging audit</code>	Enables switch auditing.	GC
<code>logging buffered</code>	Limits syslog messages displayed from an internal buffer based on severity.	GC

Command	Description	Mode^a
logging console	Limits messages logged to the console based on severity.	GC
logging facility	Configures the facility to be used in log messages.	GC
logging file	Limits syslog messages sent to the logging file based on severity.	GC
logging on	Controls error messages logging.	GC
logging snmp	Enables SNMP Set command logging.	GC
logging web-session	Enables web session logging.	GC
port	Specifies the port number of syslog messages.	L
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	PE
show syslog-servers	Displays the syslog servers settings.	PE
terminal monitor	Enables the display of logging messages on the terminal.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

System Management

Command	Description	Mode^a
asset-tag	Specifies the switch asset-tag.	GC
banner exec	Sets the message that is displayed after a successful login.	GC
banner login	Sets the message that is displayed just before the login prompt.	GC
banner motd	Specifies message-of-the-day banner.	GC
banner motd acknowledge	Acknowledges message-of-the-day banner.	GC
clear checkpoint statistics	Clears the statistics for the checkpointing process.	GC

Command	Description	Mode^a
cut-through mode	Enables the cut-through mode on the switch.	GC
exec-banner	Enables exec banner on the console, telnet or SSH connection.	LC
hostname	Specifies or modifies the switch host name.	GC
locate	Locates a switch by LED blinking.	PE
login-banner	Enables login banner on the console, telnet, or SSH connection.	LC
media-type	Selects the media-type for the interface. This command only valid on combo ports.	IC
member	Configures the switch.	SG
motd-banner	Enables motd on the console, telnet, or SSH connection.	LC
ping	Sends ICMP echo request packets to another node on the network.	UE
reload	Reloads the operating system.	PE
set description	Associates a text description with a switch in the stack.	SG
slot	Configures a slot in the system.	GC
show banner	Displays banner information.	PE
show boot-version	Displays the boot image version details.	UE
show checkpoint statistics	Displays the statistics for the checkpointing process.	PE
show cut-through mode	Show the cut-through mode on the switch.	PE
show interfaces advanced firmware	Displays the firmware revision of the PHY for a port.	PE
show memory cpu	Checks the total and available RAM space on the switch.	PE
show power-usage-history	Shows the history of unit power consumption for the unit specified in the command and total stack power consumption.	PE

Command	Description	Mode^a
<code>show process cpu</code>	Checks the CPU utilization for each process currently running on the switch.	PE
<code>show sessions</code>	Displays a list of the open telnet sessions to remote hosts.	PE
<code>show slot</code>	Displays information about all the slots in the system or for a specific slot.	UE
<code>show supported cardtype</code>	Displays information about all card types supported in the system.	UE
<code>show supported switchtype</code>	Displays information about all supported switch types.	UE
<code>show switch</code>	Displays information about the switch status.	UE
<code>show system</code>	Displays system information.	UE
<code>show system fan</code>	Explicitly displays the fan status.	UE or PE
<code>show system id</code>	Displays the service ID information.	UE
<code>show system power</code>	Displays information about the system level power consumption.	UE or PE
<code>show system temperature</code>	Displays information about the system temperature and fan status.	UE or PE
<code>show tech-support</code>	Displays system and configuration information (for debugging/calls to technical support).	PE
<code>show users</code>	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.	PE
<code>show version</code>	Displays the system version information.	UE
<code>stack</code>	Sets the mode to Stack Global Configuration mode.	GC
<code>telnet</code>	Logs into a host that supports Telnet.	PE
<code>tracert</code>	Discovers the IP routes that packets actually take when travelling to their destinations.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Telnet Server

Command	Description	Mode ^a
<code>ip telnet server disable</code>	Enables/disables the Telnet service on the switch.	GC
<code>ip telnet port</code>	Configures the Telnet TCP port number on the switch.	GC
<code>show ip telnet</code>	Displays the status of the Telnet server and the Telnet TCP port number.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Terminal Length

Command	Description	Mode ^a
<code>terminal length</code>	Sets the terminal length.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Time Ranges

Command	Description	Mode ^a
<code>time-range</code>	Creates a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries.	GC
<code>absolute</code>	Adds an absolute time entry to a time range.	TRC
<code>periodic</code>	Adds a periodic time entry to a time range.	TRC
<code>show time-range</code>	Displays a time range and all the absolute/periodic time entries that are defined for the time range.	PE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

USB Flash Drive

Command	Description	Mode ^a
<code>unmount usb</code>	Makes the USB flash device inactive.	PE
<code>show usb</code>	Displays the USB flash device details.	PE
<code>dir usb</code>	Displays the USB device contents and memory statistics.	PE

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

User Interface

Command	Description	Mode ^a
<code>enable</code>	Enters the privileged EXEC mode.	UE
<code>end</code>	Gets the CLI user control back to the privileged execution mode or user execution mode.	Any
<code>exit</code>	Exits any configuration mode to the previously highest mode in the CLI mode hierarchy.	(All)
<code>exit (EXEC)</code>	Closes an active terminal session by logging off the switch.	UE
<code>quit</code>	Closes an active terminal session by logging off the switch.	UE

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Web Server

Command	Description	Mode ^a
<code>common-name</code>	Specifies the common-name for the device.	CC
<code>country</code>	Specifies the country.	CC
<code>crypto certificate generate</code>	Generates a HTTPS certificate.	GC
<code>crypto certificate import</code>	Imports a certificate signed by the Certification Authority for HTTPS.	GC
<code>crypto certificate request</code>	Generates and displays a certificate request for HTTPS.	PE
<code>duration</code>	Specifies the duration in days.	CC

Command	Description	Mode^a
<code>ip http port</code>	Specifies the TCP port for use by a web browser to configure the switch.	GC
<code>ip http server</code>	Enables the switch to be configured from a browser.	GC
<code>ip http secure-certificate</code>	Configures the active certificate for HTTPS.	GC
<code>ip http secure-port</code>	Configures a TCP port for use by a secure web browser to configure the switch.	GC
<code>ip http secure-server</code>	Enables the switch to be configured, monitored, or modified securely from a browser.	GC
<code>key-generate</code>	Specifies the key-generate.	CC
<code>location</code>	Specifies the location or city name.	CC
<code>organization-unit</code>	Specifies the organization-unit or department name.	CC
<code>show crypto certificate mycertificate</code>	Displays the SSL certificates of your switch.	PE
<code>show ip http server status</code>	Displays the HTTP server status information.	PE
<code>show ip http server secure status</code>	Displays the HTTP secure server status information.	UE or PE
<code>state</code>	Specifies the state or province name.	CC

a. For the meaning of each Mode abbreviation, see [Mode Types](#) on page 81.

Using the CLI

Introduction

This chapter describes the basics of entering and editing the Dell PowerConnect 70xx 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 chapter 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** 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](#)
- [Operating on Multiple Objects \(Range\)](#)
- [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.

Table 2-1. History Buffer

Keyword	Source or Destination
Up-arrow key <Ctrl> + <P>	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key <Ctrl> + <N>	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence recalls more recent commands in succession.

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 on page 1541 in the Line command mode chapter 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. 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), config mode, interface config mode and all config submodes such as VLAN database config mode, and interface config mode with command completion.

Example:

```
console>en
console#configure
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#show interface status
Port    Name                Duplex Speed  Neg  Link Flow Control
                State Status
```

Gi1/0/1	N/A	Unknown	Auto	Down	Inactive
Gi1/0/2	N/A	Unknown	Auto	Down	Inactive
Gi1/0/3	N/A	Unknown	Auto	Down	Inactive
Gi1/0/4	N/A	Unknown	Auto	Down	Inactive
Gi1/0/5	N/A	Unknown	Auto	Down	Inactive
Gi1/0/6	N/A	Unknown	Auto	Down	Inactive

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 short cuts.

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

Table 2-2. CLI Shortcuts

Keyboard Key	Description
<Delete, Backspace>	Delete previous character
<Ctrl>+<A>	Go to beginning of line
<Ctrl>+<E>	Go to end of line
<Ctrl>+<F>	Go forward one character
<Ctrl>+	Go backward one character
<Ctrl>+<D>	Delete current character
<Ctrl>+<U,X>	Delete to beginning of line
<Ctrl>+<K>	Delete to the end of the line.
<Ctrl>+<W>	Delete previous word
<Ctrl>+<T>	Transpose previous character
<Ctrl>+<P>	Go to previous line history buffer
<Ctrl>+<R>	Rewrites or pastes the line
<Ctrl>+<N>	Go to next line in history buffer
<Ctrl>+<Y>	Print last deleted character
<Ctrl>+<Q>	Enables serial flow
<Ctrl>+<S>	Disables serial flow
<Ctrl>+<Z>	Return to root command prompt
<Tab, SPACE>	Command-line completion
end	Return to the root command prompt
exit	Go to next lower command prompt
<?>	List choices

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.

Operating on Multiple Objects (Range)

The CLI allows the user to operate on the set of objects at the same time. The guidelines are as follows for range operation:

- Operations on objects with four or more instances support the range operation, unless noted otherwise in the specific command documentation.
- The **range** key word is used to identify the range of objects on which to operate.
- The range may be specified in the following manner:

(**#-#**) — a range from a particular instance to another instance (inclusive). For example, 1/0/1-10 indicates that the operation applies to the gigabit Ethernet ports 1 to 10 on unit 1.

(**#, #, #**) — a list of non-consecutive instances. For example, (1/0/1, 1/0/1,1/0/3, 1/0/5) indicates that the operation applies to the gigabit Ethernet ports 1, 3, and 5 on unit 1.

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



NOTE: Each port must be a fully qualified port identifier in the format *unit/slot/port*. See [Interface Naming Conventions](#) on page 174.

- To specify a range of LAGs, use the following command:
interface range port-channel 1-48
- 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 gi1/0/2,gi1/0/4 respectively.
- When operating on a range of objects, 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.

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

Convention	Description
[]	In a command line, square brackets indicate an optional entry.
{ }	In a command line inclusive brackets indicate a selection of compulsory parameters separated by the character. One option must be selected. For example: <code>flowcontrol {auto on off}</code> means that for the <code>flowcontrol</code> command either <code>auto</code> , <code>on</code> or <code>off</code> must be selected.
<i>Italic</i>	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

The gigabit Ethernet and ten-gigabit Ethernet ports 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 port 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#* — Is the slot number for blade products that connect to a chassis. Certain interfaces have more than one slot. For example, a 10G plug-in module may have two slots, each with two ports. Slot numbers range from 0 to one minus the maximum number of slots available on the switch. The slot value is 0 for non-blade switches.
- *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, typically 24 or 48.

Within this document, the tag *interface-id* refers to an interface identifier that follows the naming convention above.

Table 2-4. Interface Identifiers

Interface Type	Long Form	Short Form	Identifier
Fast Ethernet	fastethernet	fa	unit/slot/port
Gigabit Ethernet	gigabitethernet	gi	unit/slot/port
10-Gigabit Ethernet	tengigabitethernet	te	unit/slot/port
40-Gigabit Ethernet	fortygigabitethernet	fo	unit/slot/port
Loopback	loopback	lo	loopback-id (0-7)
Port Channel	port-channel	po	port-channel-number
Tunnel	tunnel	tu	tunnel-id (0-7)
Vlan	vlan	vl	vlan-id (1-4093)

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.

Port Channel Interfaces

Port-channel (or LAG) interfaces are represented in the CLI by the variable *port-channel-number*, which can assume values from 1-128 on most PowerConnect switches.

When listed in command line output, port channel interfaces are preceded by the characters *Po*.

Loopback Interfaces

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

VLAN Interfaces

VLAN interfaces are represented in the CLI by the variable *vlan-id*, which can assume values from 1-4093.

Tunnel Interfaces

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

Examples

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
vl 5
```

Example #2

```
console#show vlan
```

VLAN	Name	Ports	Type
1	default	Po1-48, Gi1/0/1-24	Default

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 three categories:

- Layer 2 (Data Link Layer) commands
- Layer 3 (Network Layer) commands
- Utility Commands

Layer 2 (Data Link Layer) describes the logical organization of data bits transmitted on a particular medium. This layer defines the framing, addressing and checksumming of Ethernet packets.

Layer 3 (Network Layer) describes how a series of exchanges over various data links can deliver data between any two nodes in a network. This layer defines the addressing and routing structure of the Internet.

Utility 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 Configuration sub tree.

There are levels beneath the 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. 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, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode provides access to commands that can not be executed in the User EXEC mode and permits access to the switch Configuration mode.

The Global Configuration mode manages switch configuration on a global level. For specific interface configurations, command modes exist at a sub-level.

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 the Global Configuration mode.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is 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.

```
console#
```

Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC mode command `configure` is used to enter the Global Configuration mode.

```
console (config) #
```

The following are the Global Configuration modes:

- **SNMP v3 Host Configuration** — Configures the parameters for the SNMP v3 server host.
- **SNMP Community Configuration** — Configures the parameters for the SNMP server community.

Interface and Other Specific Configuration Modes

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

- **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.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The Global Configuration mode command `vlan database` is used to enter the VLAN Database 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.
- **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.
- **Ethernet** — Contains commands to manage Ethernet port configuration. The Global Configuration mode command **interface** 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 an 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.
- **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. The SSH Public-Key Chain Configuration mode command **user-key** command is used to enter the SSH Public-Key Configuration mode.
- **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.
- **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 log server.
- **Datacenter-Bridging** — Contains priority-flow-control commands. The datacenter-bridging command for an ethernet or port-channel interface is used to enter the DataCenterBridging mode.

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, 1/0/1).

[# | >] — 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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
User EXEC	The user is automatically in User EXEC mode unless the user is defined as a privileged user.	console>	logout
Privileged EXEC	Use the enable command to enter into this mode. This mode is password protected.	console#	Use the exit command, or press <Ctrl> + <Z> to return to the User EXEC mode.
Global Configuration	From Privileged EXEC mode, use the configure command.	console(config)#	Use the exit command, or press <Ctrl> + <Z> to return to the Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Line Interface	From Global Configuration mode, use the line command.	console(config-line)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Management Access-List	From Global Configuration mode, use the management access-list command.	console(config-macal)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Policy-Class-Map	From Global Configuration mode, use the policy-map class command.	console(config-policy-classmap)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Class-Map	From Global Configuration mode, use the class-map command.	console(config-classmap)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
MAC Access List	From Global Configuration mode, use the mac access-list command.	console(config-mac-access-list)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SSH Public Key-Chain	From Global Configuration mode, use the crypto key pubkey-chain ssh command.	console(config-pubkey-chain)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SSH Public Key String	From the SSH Public Key- Chain mode, use the user-key <user name> {rsa dsa} command.	console(config-pubkey-key)#	To return to the SSH Public key-chain mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
TACACS	From Global Configuration mode, use the tacacs-server host command.	console(tacacs)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Radius	From Global Configuration mode, use the radius-server host command.	console(config-radius)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP Host Configuration	From Global Configuration mode, use the snmp-server command.	console(config-snmp)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP v3 Host Configuration	From Global Configuration mode, use the snmp-server v3-host command.	console(config-snmp)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP Community Configuration	From Global Configuration mode, use the snmp-server community command.	console(config-snmp)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Crypto Certificate Generation	From Global Configuration mode, use the crypto certificate number generate command.	console(config-crypto-cert)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Crypto Certificate Request	From Privileged EXEC mode, use the crypto certificate number request command.	console(config-crypto-cert)#	To exit to Privileged EXEC mode, use the exit command, or press <Ctrl> + <Z>.
Stack	From Global Configuration mode, use the stack command.	console(config-stack)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Logging	From Global Configuration mode, use the logging command.	console(config-logging)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
MST	From Global Configuration mode, use the spanning-tree mst configuration command.	console(config-mst)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
VLAN Config	From Global Configuration mode, use the vlan database command.	console(config-vlan)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Router OSPF Conf	From Global Configuration mode, use the router ospf command.	console(config-router)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
Router RIP Config	From Global Configuration mode, use the router rip command.	console(config-router)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Router OSPFv3 Config	From Global Configuration mode, use the ipv6 router ospf command.	console(config-rtr)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
IPv6 DHCP Pool Mode	From Global Configuration mode, use the ipv6 dhcp pool command.	console(config-dhcp6-pool)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
Interface Configuration Modes			
Gigabit Ethernet	From Global Configuration mode, use the interface gigabitethernet command. Or, use the abbreviation interface gi .	console (config-if-Giunit/slot/port#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
10 Gigabit Ethernet	From Global Configuration mode, use the interface tengigabitethernet command. Or, use the abbreviation interface te .	console (config-if-Teunit/slot/port#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
40 Gigabit Ethernet	From Global Configuration mode, use the interface fortygigabitethernet command. Or, use the abbreviation interface fo .	console (config-if- <i>Founit/slot/port</i>)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Port Channel	From Global Configuration mode, use the interface port-channel command. Or, use the abbreviation interface po .	console (config-if-po <i>port-channel-number</i>)#	To exit to Global Configuration mode, use the exit command, or <Ctrl> + <Z> to Privileged EXEC mode.
VLAN	From Global Configuration mode, use the interface vlan command.	console (config-if-vlan <i>vlan-id</i>)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Tunnel	From Global Configuration mode, use the interface tunnel command. Or, use the abbreviation interface tu .	console (config-tunnel <i>tunnel-id</i>)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

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

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Loopback	From Global configuration mode, use the interface loopback command. Or, use the abbreviation interface lo .	console(config-loopback <code>loopback-id</code>)#	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

Starting the CLI

To begin running the CLI, perform the following steps:



NOTE: This procedure is for use on the console line only.



NOTE: The Easy Setup Wizard is available only when the system is in default state with no user configuration saved previously.

- 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 using the Easy Setup Wizard and enter the necessary commands to complete the required tasks.
- 3 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.

Easy Setup Wizard

The Easy Setup Wizard guides the user in the basic initial configuration of a newly installed switch so that it can be immediately deployed and functional in its basic operation and be completely manageable through the Web, CLI and the remote Dell Network Manager. After initial setup, the user may enter to the system to set up more advanced configurations.

By default the switch is shipped from the factory with an IP address of 192.168.2.1 but the Easy Setup Wizard provides the opportunity to customize the IP address. The initial activation must be done using the serial interface since, without a unique IP address, the user can not access the other management interfaces.

The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the setup. The user may return to add users later. The initial account is given the highest privilege level (level 15).
- Enables CLI login and HTTP access to use the local authentication setting only, which allows user account access via these management interfaces. The user may return later to configure Radius or TACACS+.
- Sets the IP address for VLAN 1 or enables support for DHCP to configure the IP address dynamically.
- Sets up the SNMP community string to be used by the SNMP manager. The user may choose to skip this step if SNMP management is not used. If it is configured, the default access level is set to the highest available access for the SNMP management interface. The user may return later to add to the community string or reconfigure the access level of the community string. Initially only SNMPv1/2c will be activated. SNMPv3 is disabled until the user returns to configure security access for SNMPv3 (for example, engine ID, view, and so on). The SNMP community string may include spaces. The wizard requires the use of quotation marks when the user wants to enter spaces in the community string. Although spaces are allowed in the community string, their use is discouraged. The default community string contains no spaces.
- Allows the user to specify the management server IP or permit SNMP access from all IP addresses.
- Sets up the default gateway IP address.

If the user chooses not to use the wizard initially, the session defaults to the CLI mode with a warning to refer the documentation. During a subsequent login, the user may again elect not to run the setup wizard. Once the wizard has established configuration, however, the wizard is presented only if the user resets the switch to the factory default settings. While the wizard is

running, the system does not display any unsolicited or unrelated status messages. For example, the system does not display event notification or system status messages.

After completing the wizard, the user is given a chance to save his configuration and continue to the CLI. If the user chooses to discard his configuration, any restart of the wizard must be from the beginning. When the user chooses to restart the wizard, any configuration the user saved previously automatically is offered for the user to accept. The user may elect to correct only a few items instead of re-entering all the data.

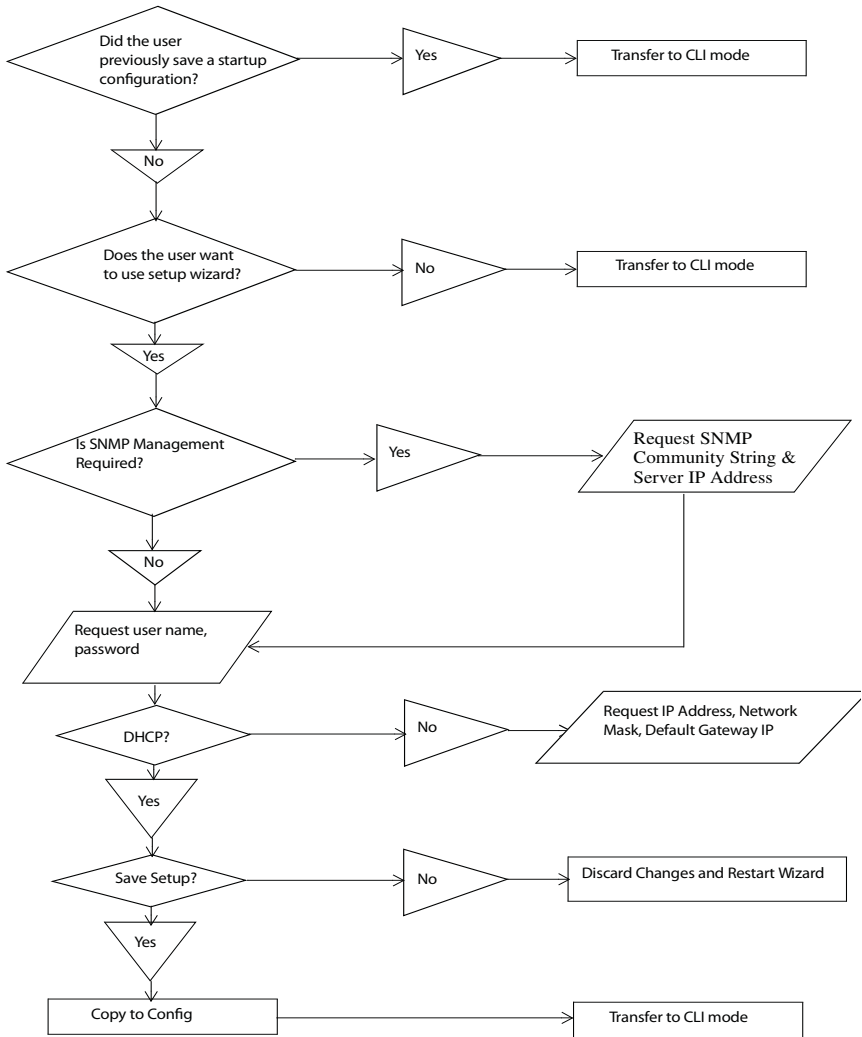
Since a switch may be powered on in the field without a serial connection, the switch waits 60 seconds for the user to respond to the setup wizard question in instances where no configuration files exist. If there is no response, the switch continues normal operation using the default factory configuration. While waiting for the response from the user, normal switch operation will continue, including but not limited to:

- If BOOTP/DHCP is supported and enabled by default, the switch attempts to get its address.
- The switch continues to switch traffic.
- The switch continues do MAC learning. If spanning-tree is on by default, the switch participates in the spanning-tree protocol.

Functional Flow

The functional flow diagram in Figure 2-1 illustrates the procedures for the Easy Setup Wizard.

Figure 2-1. Easy Setup Wizard



Example Session

This section describes an Easy Setup Wizard session. Refer to the state diagram in the previous section for general flow. The following values used by the example session are not the only possible ones:

- IP address for the VLAN 1 is 192.168.1.2:255.255.255.0. This address is on a different subnet than the OOB interface and in the same subnet as the default gateway.
- The user name is *admin*, and the password should be 8-64 characters in length (admin123).
- The network management system IP address is 192.168.2.1.
- The default gateway is 0.0.0.0.
- The SNMP community string to be used is *public*.

The setup wizard configures the initial values as defined above. After the user completes the wizard, the system is configured as follows:

- SNMPv1/2c is enabled and the community string is set up as defined above. SNMPv3 is disabled.
- The admin user account is set up as defined.
- The address of the network management station is configured. From this management station, the user can access the SNMP, HTTP, and CLI interfaces. The user may also choose to allow all IP addresses to access switch management by choosing the (0.0.0.0) IP address.
- An IP address is configured for the default VLAN (1).
- A default gateway address is configured.

The following example contains the sequence of prompts and responses associated with running an example Dell Easy Setup Wizard session, using the input values listed above. Note in this case a static IP address for the management interface is being set up. However it may be requested that the system automatically retrieve an IP address via DHCP. If DHCP is used, the system does not request a network mask or default gateway. In this example, the user employs the setup wizard to configure the initial values as defined above.



NOTE: In the following Easy Setup Wizard example, the possible user options are enclosed in []. Also, where possible, default values are enclosed in []. If the user enters <Return> with no options defined, the default value is accepted. Help text is in parentheses.

After the switch completes the POST and is booted, the following dialog appears:

```
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] y
```

```
Step 1:
```

```
The system is not setup for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can:
```

- o Set up the initial SNMP version 2 account now.
- o Return later and setup other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

```
Would you like to setup the SNMP management interface now? [Y/N] y
```

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell
```

Network Manager or other management interfaces to change this setting, and to add additional management system later. For more information on adding management systems, see the user documentation.

To add a management station:

Please enter the SNMP community string to be used.

{public}:

public<Enter>

Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station.

{0.0.0.0}:

192.168.2.1<Enter>

Step 2:

Now we need to setup your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may setup other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To setup a user account:

Please enter the user name: admin<Enter>

Please enter the user password: *****<Enter>

Please reenter the user password: *****<Enter>

Step 3:

Next, an IP address is setup. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch.

Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).

To setup an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server.

192.168.1.2<Enter>

Please enter the IP subnet mask (A.B.C.D or /nn):

255.255.255.0<Enter>

Step 4:

Finally, set up the gateway. Please enter the IP address of the gateway from which this network is reachable

192.168.1.1<Enter>

This is the configuration information that has been collected:

SNMP Interface = "public"@192.168.2.1

User Account setup = admin

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Gateway = 0.0.0.0

Step 5:

If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: [Y/N]

y<Enter>

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

.....

console>

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 images, which store the configuration parameters for the switch. The system has three configuration images. One image is a memory-only image and is the current configuration image for the switch. The second image is the one that is loaded by the system when it reboots. There is one backup configuration image. The system also provides methods to back up these images to a remote system.

File System Commands

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

Table 2-6. File System Commands

Command	Description
<code>delete file</code>	Deletes file.
<code>filedescr file description</code>	Adds a description to a file (up to 20 characters can be used).
<code>copy source destination</code>	Copies a file from source file to destination file.

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 on page 1506 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 file systems using TFTP and XMODEM protocols.

- `tftp://server-name/path/filename` — identifies a file on a remote file system accessible through 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.
- `xmodem: filename` — identifies the file available on the XMODEM connection.

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.
- **image1 & image2** — These files refer to software images. One of these will be loaded when the system next reboots. Either image1 or image2 can be chosen for the next reboot using the command **boot system**.

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, the service port (out-of-band interface), or in-band interfaces. Since the serial interface requires a physical connection for access, it is used if all else fails. The serial 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 CLI generates keys for SSH locally.
- The serial session defaults to 9600 baud rate, eight data bits, non-parity and one stop bit.

User Accounts Management

The CLI provides authentication for 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 user may create five local user accounts.
- User accounts have an access level, a user name, and a user password.
- The user is able to delete the user accounts but the user will not be able to delete the last level 15 account.
- The user 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.
- The CLI allows the user 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 user can specify whether the CLI should revert to using local user 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 requirement applies only when the user is logged in through a telnet or an SSH session.
- The CLI always allows the user 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 user to log in.

User Access Control

In addition to authenticating a user, the CLI also assigns the user access to one of two security levels. Level 1 has read-only access. This level allow the user 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 and can not be modified.

If the user account is created and maintained locally, each user is given an access level at the time of account creation. If the user is authenticated through remote authentication servers, the authentication server is configured to pass the user access level to the CLI when the user is authenticated. When Radius is used, the *Vendor-Specific Option* field returns the access level for the user. 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 user determines whether remote authentication servers or locally defined user authentication accounts are used.
- If authentication servers are used, the user 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 user 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 user configures the CLI to fail login when the remote authentication servers are down, the CLI allows the user to log in to the serial interface authenticated by locally managed account data.

Syslogs

The CLI uses syslog support to send logging messages to a remote syslog server. The user configures the switch to generate all logging messages to a remote log server. If no remote log server exists, then the CLI maintains a rolling log of at most the last 1000 critical system events.

The following rules and specifications apply:

- The CLI permits the user to configure a remote syslog server to which all system logging messages are sent.
- Log messages are implementation-dependent but may contain debug messages, security or fault events.

- If a log server is not specified by the user, the CLI maintains at most the last 1000 critical system events. In this case, less important events are not recorded.

Security Logs

Security logs are maintained to record all 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 user 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 syslog is available, the CLI sends the security log records to the syslog server. If syslog is not available, the CLI records the last 1000 security log records in a log separate from the system log records itemized above. Also in this case, the CLI suppresses repeated events from the same source and instead the CLI records one event within a period of time and includes that count as part of the log.

Management ACL

In addition to user access control, the system also manages access for in-band interfaces. The system allows individual hosts or subnets to access only specific management protocols.

The user 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 user defines the list of hosts or subnets from which the management profiles may be used.

Other CLI Tools and Capabilities

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

Terminal Paging

The 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-* prompt on the 25th line. The CLI waits for the user to press either <q> or any other key. If the user presses any key except <q>, the CLI shows the next page. A <q> key stops the display and returns to the CLI prompt.

Boot Message

The boot message is a system message that is not user-configurable and is displayed when the system is booting. Displayed information includes the following:

- Operational code date
- The board type
- The CPU
- Memory size

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

Boot Utility Menu

If a user is connected through the serial interface during the boot sequence, pressing the <esc> key interrupts the boot process and displays a Boot Utility Menu. Selecting item 2 displays the menu and may be typed only during the initial boot up sequence. When the system boot up is complete, typing the escape sequence *does not* display the menu.

Boot Menu 4.1.0.6

Options available

- 1 - Start operational code
- 2 - Change baud rate
- 3 - Retrieve event log using XMODEM
- 4 - Load new operational code using XMODEM
- 5 - Display operational code vital product data
- 6 - Abort boot code update
- 7 - Update boot code
- 8 - Delete backup image
- 9 - Reset the system
- 10 - Restore configuration to factory defaults (delete config files)
- 11 - Activate Backup Image
- 12 - Password Recovery Procedure
- 13 - Reformat and restore file system

[Boot Menu] 2

Select baud rate:

1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
7 - 57600
8 - 115200
0 - no change

Baud rate is not changed

[Boot Menu] 3

Sending event log, start XMODEM receive.....

File asciilog.bin Ready to SEND in binary mode

Estimated File Size 0K, 12 Sectors, 89 Bytes

Estimated transmission time 14 seconds

Send several Control-X characters to cancel before transfer starts.

[Boot Menu] 4

Ready to receive the file with XMODEM/CRC....

Ready to RECEIVE File xcode.bin in binary mode

Send several Control-X characters to cancel before transfer starts.

CKCK

[Boot Menu] 5

The following image is in the Flash File System:

```
File Name.....image2
CRC.....0x3431
(13361)
Target
Device.....0x00508548
Size.....0xc178
dc (12679388)
Number of Components.....3

Operational Code
Size.....0xa73af4 (10959604)
Operational Code Offset.....0x74
(116)
Operational Code FLASH flag.....1
Operational Code CRC.....0x20E7
Operational Compression flag.....2
(lzma)

Boot Code Version.....1
```

```
Boot Code
Size.....0x100000
(1048576)

Boot Code
Offset.....0xa73b68
(10959720)

Boot Code FLASH flag.....0
Boot Code CRC.....0x578
```

```
VPD - rel 4 ver 1 maint_lvl 0 build_num 6
      Timestamp - Mon Feb 28 16:43:14 2011

      File - PC7000_M6348v4.1.0.6.opr
```

[Boot Menu] 6

[Boot Menu] 7

Do you wish to update Boot Code and reset? (y/n) y

```
Validating image2....OK
Extracting boot code from image...CRC valid
Erasing Boot Flash.....Done.
Wrote 0x10000 bytes.
Wrote 0x20000 bytes.
Wrote 0x30000 bytes.
```

```
Wrote 0x40000 bytes.  
Wrote 0x50000 bytes.  
Wrote 0x60000 bytes.  
Wrote 0x70000 bytes.  
Wrote 0x80000 bytes.  
Wrote 0x90000 bytes.  
Wrote 0xa0000 bytes.  
Wrote 0xb0000 bytes.  
Wrote 0xc0000 bytes.  
Wrote 0xd0000 bytes.  
Wrote 0xe0000 bytes.  
Wrote 0xf0000 bytes.  
Wrote 0x100000 bytes.  
Validating Flash.....Passed  
Flash update completed.  
Rebooting...
```

```
CPU Card ID: 0x508548
```

```
CFI Probe: Found 2x16 devices in x16 mode
```

```
/DskVol// - disk check in progress ...
```

```
/DskVol// - Volume is OK
```

```
Change volume Id from 0x0 to 0x79
```

```
volume descriptor ptr (pVolDesc): 0x814cf10
```

```
XBD device block I/O handle: 0x10001
```

```
auto disk check on mount:      DOS_CHK_REPAIR
|DOS_CHK_VERB_2
volume write mode:            copyback (DOS_WRITE)
volume options:
max # of simultaneously open files:    52
file descriptors in use:              0
# of different files in use:          0
# of descriptors for deleted files:    0
# of obsolete descriptors:            0

current volume configuration:
- volume label:    NO LABEL ; (in boot sector:
)
- volume Id:      0x79
- total number of sectors:    124,408
- bytes per sector:    512
- # of sectors per cluster:  4
- # of reserved sectors:    1
- FAT entry size:      FAT16
- # of sectors per FAT copy:  122
- # of FAT table copies:    2
- # of hidden sectors:      8
- first cluster is in sector # 260
- Update last access date for open-read-close = FALSE
```

Boot Menu 4.1.0.6

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

Boot Menu 4.1.0.6

Options available

1 - Start operational code

2 - Change baud rate

3 - Retrieve event log using XMODEM

4 - Load new operational code using XMODEM

5 - Display operational code vital product data

6 - Abort boot code update

7 - Update boot code

8 - Delete backup image

9 - Reset the system

10 - Restore configuration to factory defaults (delete config files)

11 - Activate Backup Image

12 - Password Recovery Procedure

13 - Reformat and restore file system

[Boot Menu] 8

Are you SURE you want to delete: image1 ? (y/n):y
image1 deleted...

[Boot Menu] 10

Are you SURE you want to delete the configuration?
(y/n):y

[Boot Menu] 11

Backup image - image1 activated.

[Boot Menu] 12

Operational Code Date: Mon Feb 28 16:43:14 2011

Uncompressing.....

Bulk Class Driver Successfully Initialized

Adding 0 symbols for standalone.

CFI Probe: Found 2x16 devices in x16 mode

volume descriptor ptr (pVolDesc): 0x5157150

XBD device block I/O handle: 0x10001

auto disk check on mount: DOS_CHK_REPAIR
|DOS_CHK_VERB_2

volume write mode: copyback (DOS_WRITE)

volume options:

max # of simultaneously open files: 52

file descriptors in use: 0

of different files in use: 0

of descriptors for deleted files: 0

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector:)
- volume Id: 0x79
- total number of sectors: 124,408
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 122
- # of FAT table copies: 2
- # of hidden sectors: 8

- first cluster is in sector # 260
- Update last access date for open-read-close = FALSE

PCI unit 0: Dev 0xb634, Rev 0x11, Chip BCM56634_B0,
Driver BCM56634_B0

SOC unit 0 attached to PCI device BCM56634_B0

soc_reset_bcm56634_a0: TCAM PLL not locked.

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

Instantiating /download as rawFs, device = 0x20001

Formatting /download for DOSFS

Instantiating /download as rawFs, device = 0x20001

Formatting...OK.

<186> NOV 15 10:03:48 0.0.0.0-1 General[1073741072]:
bootos.c(220) 1 %% Event(0xaaaaaaaa)

Instantiating RamCP: as rawFs, device = 0x30001

Formatting RamCP: for DOSFS

Instantiating RamCP: as rawFs, device = 0x30001

Formatting...OK.

(Unit 1 - Waiting to select management unit)>USB Auto Configuration process is completed!

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 ...

console>en

console#reload

Management switch has unsaved changes.

Are you sure you want to continue? (y/n) y

Configuration Not Saved!

Are you sure you want to reload the stack? (y/n) y

Reloading all switches.

Boot Menu 4.1.0.6

CPU Card ID: 0x508548

CFI Probe: Found 2x16 devices in x16 mode

/DskVol// - disk check in progress ...

/DskVol//files

/DskVol//files/image2

/DskVol//files/boot.dim

/DskVol//files/crashdump.ct1

```
/DskVol//files/dh512.pem
/DskVol//files/dh1024.pem
/DskVol//files/ssl_cert1.pem
/DskVol//files/ssl_key1.pem
/DskVol//files/ssh_host_key
/DskVol//files/ssh_host_dsa_key
/DskVol//files/ssh_host_rsa_key
/DskVol//files/log2.bin
/DskVol//files/hpc_broad.cfg
/DskVol//files/slog0.txt
/DskVol//files/olog0.txt
/DskVol//files/ssl.rnd
```

```
/DskVol// - Volume is OK
```

```
volume descriptor ptr (pVolDesc):      0x814cf10
XBD device block I/O handle: 0x10001
auto disk check on mount:      DOS_CHK_REPAIR
|DOS_CHK_VERB_2
volume write mode:      copyback (DOS_WRITE)
volume options:
max # of simultaneously open files:      52
file descriptors in use:      0
# of different files in use:      0
# of descriptors for deleted files:      0
```

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector:
)
- volume Id: 0x79
- total number of sectors: 124,408
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 122
- # of FAT table copies: 2
- # of hidden sectors: 8
- first cluster is in sector # 260
- Update last access date for open-read-close = FALSE

Boot Menu 4.1.0.6

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

Boot Menu 4.1.0.6

Options available

- 1 - Start operational code
- 2 - Change baud rate
- 3 - Retrieve event log using XMODEM
- 4 - Load new operational code using XMODEM
- 5 - Display operational code vital product data
- 6 - Abort boot code update
- 7 - Update boot code
- 8 - Delete backup image
- 9 - Reset the system
- 10 - Restore configuration to factory defaults (delete config files)
- 11 - Activate Backup Image
- 12 - Password Recovery Procedure
- 13 - Reformat and restore file system

[Boot Menu] 13

Instantiating /RamDisk/ as rawFs, device = 0x20001

Formatting /RamDisk/ for DOSFS

Instantiating /RamDisk/ as rawFs, device = 0x20001

Formatting.../RamDisk/: file system is marked clean, skipping check

OK.

copying file /DskVol/files/image1 -> /RamDisk/image1

copying file /DskVol/files/image2 -> /RamDisk/image2

```

copying file /DskVol/files/startup-config ->
/RamDisk/startup-config

copying file /DskVol/files/vpd.bin ->
/RamDisk/vpd.bin

copying file /DskVol/files/hpc_broad.cfg ->
/RamDisk/hpc_broad.cfg

copying file /DskVol/files/boot.dim ->
/RamDisk/boot.dim

copying file /DskVol/files/dh512.pem ->
/RamDisk/dh512.pem

copying file /DskVol/files/dh1024.pem ->
/RamDisk/dh1024.pem

copying file /DskVol/files/sslt_cert1.pem ->
/RamDisk/sslt_cert1.pem

copying file /DskVol/files/sslt_key1.pem ->
/RamDisk/sslt_key1.pem

copying file /DskVol/files/ssh_host_key ->
/RamDisk/ssh_host_key

copying file /DskVol/files/ssh_host_dsa_key ->
/RamDisk/ssh_host_dsa_key

copying file /DskVol/files/ssh_host_rsa_key ->
/RamDisk/ssh_host_rsa_key

image2                                12679504    11/15/113
9:30:36

hpc_broad.cfg                          148        11/15/113
10:04:30

boot.dim                                77         4/22/105
8:00:02

dh512.pem                               156        5/30/113
0:20:24

```


dh1024.pem 0:20:24	245	5/30/113
sslt_cert1.pem 5:09:30	863	6/2/113
sslt_key1.pem 5:09:30	887	6/2/113
ssh_host_key 0:20:24	517	5/30/113
ssh_host_dsa_key 0:20:24	672	5/30/113
ssh_host_rsa_key 0:20:24	887	5/30/113

Filesystem size 25484288

Bytes used 12683956

Bytes free 12800332

Erasing FFS: CFI Probe: Found 2x16 devices in x16 mode

Formatted 1 of 251 units = 0.3 %

Formatted 2 of 251 units = 0.7 %

Formatted 3 of 251 units = 1.1 %

Formatted 4 of 251 units = 1.5 %

Formatted 5 of 251 units = 1.9 %

Formatted 6 of 251 units = 2.3 %

Formatted 7 of 251 units = 2.7 %

Formatted 8 of 251 units = 3.1 %

Formatted 9 of 251 units = 3.5 %

Formatted 10 of 251 units = 3.9 %

Formatted 11 of 251 units = 4.3 %

Formatted 12 of 251 units = 4.7 %
Formatted 13 of 251 units = 5.1 %
Formatted 14 of 251 units = 5.5 %
Formatted 15 of 251 units = 5.9 %
Formatted 16 of 251 units = 6.3 %
Formatted 17 of 251 units = 6.7 %
Formatted 18 of 251 units = 7.1 %
Formatted 19 of 251 units = 7.5 %
Formatted 20 of 251 units = 7.9 %
Formatted 21 of 251 units = 8.3 %
Formatted 22 of 251 units = 8.7 %
Formatted 23 of 251 units = 9.1 %
Formatted 24 of 251 units = 9.5 %
Formatted 25 of 251 units = 9.9 %
Formatted 26 of 251 units = 10.3 %
Formatted 27 of 251 units = 10.7 %
Formatted 28 of 251 units = 11.1 %
Formatted 29 of 251 units = 11.5 %
Formatted 30 of 251 units = 11.9 %
Formatted 31 of 251 units = 12.3 %
Formatted 32 of 251 units = 12.7 %
Formatted 33 of 251 units = 13.1 %
Formatted 34 of 251 units = 13.5 %
Formatted 35 of 251 units = 13.9 %
Formatted 36 of 251 units = 14.3 %
Formatted 37 of 251 units = 14.7 %

Formatted 38 of 251 units = 15.1 %
Formatted 39 of 251 units = 15.5 %
Formatted 40 of 251 units = 15.9 %
Formatted 41 of 251 units = 16.3 %
Formatted 42 of 251 units = 16.7 %
Formatted 43 of 251 units = 17.1 %
Formatted 44 of 251 units = 17.5 %
Formatted 45 of 251 units = 17.9 %
Formatted 46 of 251 units = 18.3 %
Formatted 47 of 251 units = 18.7 %
Formatted 48 of 251 units = 19.1 %
Formatted 49 of 251 units = 19.5 %
Formatted 50 of 251 units = 19.9 %
Formatted 51 of 251 units = 20.3 %
Formatted 52 of 251 units = 20.7 %
Formatted 53 of 251 units = 21.1 %
Formatted 54 of 251 units = 21.5 %
Formatted 55 of 251 units = 21.9 %
Formatted 56 of 251 units = 22.3 %
Formatted 57 of 251 units = 22.7 %
Formatted 58 of 251 units = 23.1 %
Formatted 59 of 251 units = 23.5 %
Formatted 60 of 251 units = 23.9 %
Formatted 61 of 251 units = 24.3 %
Formatted 62 of 251 units = 24.7 %
Formatted 63 of 251 units = 25.0 %

Formatted 64 of 251 units = 25.4 %
Formatted 65 of 251 units = 25.8 %
Formatted 66 of 251 units = 26.2 %
Formatted 67 of 251 units = 26.6 %
Formatted 68 of 251 units = 27.0 %
Formatted 69 of 251 units = 27.4 %
Formatted 70 of 251 units = 27.8 %
Formatted 71 of 251 units = 28.2 %
Formatted 72 of 251 units = 28.6 %
Formatted 73 of 251 units = 29.0 %
Formatted 74 of 251 units = 29.4 %
Formatted 75 of 251 units = 29.8 %
Formatted 76 of 251 units = 30.2 %
Formatted 77 of 251 units = 30.6 %
Formatted 78 of 251 units = 31.0 %
Formatted 79 of 251 units = 31.4 %
Formatted 80 of 251 units = 31.8 %
Formatted 81 of 251 units = 32.2 %
Formatted 82 of 251 units = 32.6 %
Formatted 83 of 251 units = 33.0 %
Formatted 84 of 251 units = 33.4 %
Formatted 85 of 251 units = 33.8 %
Formatted 86 of 251 units = 34.2 %
Formatted 87 of 251 units = 34.6 %
Formatted 88 of 251 units = 35.0 %
Formatted 89 of 251 units = 35.4 %

Formatted 90 of 251 units = 35.8 %
Formatted 91 of 251 units = 36.2 %
Formatted 92 of 251 units = 36.6 %
Formatted 93 of 251 units = 37.0 %
Formatted 94 of 251 units = 37.4 %
Formatted 95 of 251 units = 37.8 %
Formatted 96 of 251 units = 38.2 %
Formatted 97 of 251 units = 38.6 %
Formatted 98 of 251 units = 39.0 %
Formatted 99 of 251 units = 39.4 %
Formatted 100 of 251 units = 39.8 %
Formatted 101 of 251 units = 40.2 %
Formatted 102 of 251 units = 40.6 %
Formatted 103 of 251 units = 41.0 %
Formatted 104 of 251 units = 41.4 %
Formatted 105 of 251 units = 41.8 %
Formatted 106 of 251 units = 42.2 %
Formatted 107 of 251 units = 42.6 %
Formatted 108 of 251 units = 43.0 %
Formatted 109 of 251 units = 43.4 %
Formatted 110 of 251 units = 43.8 %
Formatted 111 of 251 units = 44.2 %
Formatted 112 of 251 units = 44.6 %
Formatted 113 of 251 units = 45.0 %
Formatted 114 of 251 units = 45.4 %
Formatted 115 of 251 units = 45.8 %

Formatted 116 of 251 units = 46.2 %
Formatted 117 of 251 units = 46.6 %
Formatted 118 of 251 units = 47.0 %
Formatted 119 of 251 units = 47.4 %
Formatted 120 of 251 units = 47.8 %
Formatted 121 of 251 units = 48.2 %
Formatted 122 of 251 units = 48.6 %
Formatted 123 of 251 units = 49.0 %
Formatted 124 of 251 units = 49.4 %
Formatted 125 of 251 units = 49.8 %
Formatted 126 of 251 units = 50.1 %
Formatted 127 of 251 units = 50.5 %
Formatted 128 of 251 units = 50.9 %
Formatted 129 of 251 units = 51.3 %
Formatted 130 of 251 units = 51.7 %
Formatted 131 of 251 units = 52.1 %
Formatted 132 of 251 units = 52.5 %
Formatted 133 of 251 units = 52.9 %
Formatted 134 of 251 units = 53.3 %
Formatted 135 of 251 units = 53.7 %
Formatted 136 of 251 units = 54.1 %
Formatted 137 of 251 units = 54.5 %
Formatted 138 of 251 units = 54.9 %
Formatted 139 of 251 units = 55.3 %
Formatted 140 of 251 units = 55.7 %
Formatted 141 of 251 units = 56.1 %

Formatted 142 of 251 units = 56.5 %
Formatted 143 of 251 units = 56.9 %
Formatted 144 of 251 units = 57.3 %
Formatted 145 of 251 units = 57.7 %
Formatted 146 of 251 units = 58.1 %
Formatted 147 of 251 units = 58.5 %
Formatted 148 of 251 units = 58.9 %
Formatted 149 of 251 units = 59.3 %
Formatted 150 of 251 units = 59.7 %
Formatted 151 of 251 units = 60.1 %
Formatted 152 of 251 units = 60.5 %
Formatted 153 of 251 units = 60.9 %
Formatted 154 of 251 units = 61.3 %
Formatted 155 of 251 units = 61.7 %
Formatted 156 of 251 units = 62.1 %
Formatted 157 of 251 units = 62.5 %
Formatted 158 of 251 units = 62.9 %
Formatted 159 of 251 units = 63.3 %
Formatted 160 of 251 units = 63.7 %
Formatted 161 of 251 units = 64.1 %
Formatted 162 of 251 units = 64.5 %
Formatted 163 of 251 units = 64.9 %
Formatted 164 of 251 units = 65.3 %
Formatted 165 of 251 units = 65.7 %
Formatted 166 of 251 units = 66.1 %
Formatted 167 of 251 units = 66.5 %

Formatted 168 of 251 units = 66.9 %
Formatted 169 of 251 units = 67.3 %
Formatted 170 of 251 units = 67.7 %
Formatted 171 of 251 units = 68.1 %
Formatted 172 of 251 units = 68.5 %
Formatted 173 of 251 units = 68.9 %
Formatted 174 of 251 units = 69.3 %
Formatted 175 of 251 units = 69.7 %
Formatted 176 of 251 units = 70.1 %
Formatted 177 of 251 units = 70.5 %
Formatted 178 of 251 units = 70.9 %
Formatted 179 of 251 units = 71.3 %
Formatted 180 of 251 units = 71.7 %
Formatted 181 of 251 units = 72.1 %
Formatted 182 of 251 units = 72.5 %
Formatted 183 of 251 units = 72.9 %
Formatted 184 of 251 units = 73.3 %
Formatted 185 of 251 units = 73.7 %
Formatted 186 of 251 units = 74.1 %
Formatted 187 of 251 units = 74.5 %
Formatted 188 of 251 units = 74.9 %
Formatted 189 of 251 units = 75.2 %
Formatted 190 of 251 units = 75.6 %
Formatted 191 of 251 units = 76.0 %
Formatted 192 of 251 units = 76.4 %
Formatted 193 of 251 units = 76.8 %

Formatted 194 of 251 units = 77.2 %
Formatted 195 of 251 units = 77.6 %
Formatted 196 of 251 units = 78.0 %
Formatted 197 of 251 units = 78.4 %
Formatted 198 of 251 units = 78.8 %
Formatted 199 of 251 units = 79.2 %
Formatted 200 of 251 units = 79.6 %
Formatted 201 of 251 units = 80.0 %
Formatted 202 of 251 units = 80.4 %
Formatted 203 of 251 units = 80.8 %
Formatted 204 of 251 units = 81.2 %
Formatted 205 of 251 units = 81.6 %
Formatted 206 of 251 units = 82.0 %
Formatted 207 of 251 units = 82.4 %
Formatted 208 of 251 units = 82.8 %
Formatted 209 of 251 units = 83.2 %
Formatted 210 of 251 units = 83.6 %
Formatted 211 of 251 units = 84.0 %
Formatted 212 of 251 units = 84.4 %
Formatted 213 of 251 units = 84.8 %
Formatted 214 of 251 units = 85.2 %
Formatted 215 of 251 units = 85.6 %
Formatted 216 of 251 units = 86.0 %
Formatted 217 of 251 units = 86.4 %
Formatted 218 of 251 units = 86.8 %
Formatted 219 of 251 units = 87.2 %

Formatted 220 of 251 units = 87.6 %
Formatted 221 of 251 units = 88.0 %
Formatted 222 of 251 units = 88.4 %
Formatted 223 of 251 units = 88.8 %
Formatted 224 of 251 units = 89.2 %
Formatted 225 of 251 units = 89.6 %
Formatted 226 of 251 units = 90.0 %
Formatted 227 of 251 units = 90.4 %
Formatted 228 of 251 units = 90.8 %
Formatted 229 of 251 units = 91.2 %
Formatted 230 of 251 units = 91.6 %
Formatted 231 of 251 units = 92.0 %
Formatted 232 of 251 units = 92.4 %
Formatted 233 of 251 units = 92.8 %
Formatted 234 of 251 units = 93.2 %
Formatted 235 of 251 units = 93.6 %
Formatted 236 of 251 units = 94.0 %
Formatted 237 of 251 units = 94.4 %
Formatted 238 of 251 units = 94.8 %
Formatted 239 of 251 units = 95.2 %
Formatted 240 of 251 units = 95.6 %
Formatted 241 of 251 units = 96.0 %
Formatted 242 of 251 units = 96.4 %
Formatted 243 of 251 units = 96.8 %
Formatted 244 of 251 units = 97.2 %
Formatted 245 of 251 units = 97.6 %

Formatted 246 of 251 units = 98.0 %
Formatted 247 of 251 units = 98.4 %
Formatted 248 of 251 units = 98.8 %
Formatted 249 of 251 units = 99.2 %
Formatted 250 of 251 units = 99.6 %
Formatted 251 of 251 units = 100.0 %

CFI Probe: Found 2x16 devices in x16 mode

Recreating FFS: CFI Probe: Found 2x16 devices in x16 mode

/DskVol/: file system is marked clean, skipping check

volume descriptor ptr (pVolDesc): 0x9a67710
XBD device block I/O handle: 0x40001
auto disk check on mount: DOS_CHK_REPAIR
|DOS_CHK_VERB_2
volume write mode: copyback (DOS_WRITE)
volume options:
max # of simultaneously open files: 52
file descriptors in use: 0
of different files in use: 0
of descriptors for deleted files: 0
of obsolete descriptors: 0

current volume configuration:

```
- volume label:    NO LABEL ; (in boot sector:
)
- volume Id:      0x0
- total number of sectors:    124,408
- bytes per sector:    512
- # of sectors per cluster: 4
- # of reserved sectors:    1
- FAT entry size:    FAT16
- # of sectors per FAT copy:    122
- # of FAT table copies:    2
- # of hidden sectors:    8
- first cluster is in sector # 260
- Update last access date for open-read-close = FALSE
```

done

.
..

Filesystem size 63567872

Bytes used 0

Bytes free 63567872

copying file /RamDisk/image1 -> /DskVol/files/image1

copying file /RamDisk/image2 -> /DskVol/files/image2

```

copying file /RamDisk/startup-config ->
/DskVol/files/startup-config
copying file /RamDisk/vpd.bin ->
/DskVol/files/vpd.bin
copying file /RamDisk/hpc_broad.cfg ->
/DskVol/files/hpc_broad.cfg
copying file /RamDisk/boot.dim ->
/DskVol/files/boot.dim
copying file /RamDisk/dh512.pem ->
/DskVol/files/dh512.pem
copying file /RamDisk/dh1024.pem ->
/DskVol/files/dh1024.pem
copying file /RamDisk/sslt_cert1.pem ->
/DskVol/files/sslt_cert1.pem
copying file /RamDisk/sslt_key1.pem ->
/DskVol/files/sslt_key1.pem
copying file /RamDisk/ssh_host_key ->
/DskVol/files/ssh_host_key
copying file /RamDisk/ssh_host_dsa_key ->
/DskVol/files/ssh_host_dsa_key
copying file /RamDisk/ssh_host_rsa_key ->
/DskVol/files/ssh_host_rsa_key
.
..
image2                               12679504   11/15/113
9:30:36
hpc_broad.cfg                         148       11/15/113
10:04:30
boot.dim                               77        4/22/105
8:00:02

```

dh512.pem 0:20:24	156	5/30/113
dh1024.pem 0:20:24	245	5/30/113
sslt_cert1.pem 5:09:30	863	6/2/113
sslt_key1.pem 5:09:30	887	6/2/113
ssh_host_key 0:20:24	517	5/30/113
ssh_host_dsa_key 0:20:24	672	5/30/113
ssh_host_rsa_key 0:20:24	887	5/30/113

Filesystem size 63567872

Bytes used 12683956

Bytes free 50883916

[Boot Menu]

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 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.

Layer 2 Switching Commands

The chapters 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:

AAA Commands	E-mail Alerting Commands	IPv6 MLD Snooping Commands	Port Monitor Commands
ACL Commands	Ethernet Configuration Commands	IPv6 MLD Snooping Querier Commands	QoS Commands
Address Table Commands	Ethernet CFM Commands	IP Source Guard Commands	RADIUS Commands
Auto-VoIP Commands	–	iSCSI Optimization Commands	Spanning Tree Commands
CDP Interoperability Commands	GVRP Commands	Link Dependency Commands	TACACS+ Commands
DHCP Layer 2 Relay Commands	IGMP Snooping Commands	LLDP Commands	VLAN Commands
DHCP Management Interface Commands	IGMP Snooping Querier Commands	Multicast VLAN Registration Commands	Voice VLAN Commands
DHCP Snooping Commands	IP Addressing Commands	–	802.1x Commands
Dynamic ARP Inspection Commands	IPv6 Access List Commands	Port Channel Commands	–

AAA Commands

Management access to the switch is via telnet, HTTP, SSH, or the serial console (SNMP access is discussed in [SNMP Commands](#)). To ensure that only authorized users can access and change the configuration of the switch, users must be authenticated.

Users can be authenticated based on:

- Login mode
- Switch access method
- Access to Privileged EXEC mode
- Two levels of access:
 - 1 = Read-only
 - 15 = Write-only

The supported authentication methods for 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 user, 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 users and components.

The administrator can enable/disable/reorder authentication methods on a per method basis (see above).

TACACS+ Accounting

The administrator may choose to account user 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.

User 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 user logs into the switch and when the user logs out of the exec mode. Accounting notifications are also sent at the beginning and at the end of the user 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 user logs out of the exec mode. The duration of the exec session is mentioned in the accounting notice.

Accounting notifications are sent at the end of each user 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. 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 config modes.

The following default Accounting Methods List are available.

Default List Name	Accounting Type	Record Type	Accounting Method
Default Exec List	exec	Start-stop	TACACS+
Default Command List	commands	Stop-only	TACACS+

The default lists are not applied to any line-configuration modes by default.

Commands in this Chapter

This chapter explains the following commands:

<code>aaa authentication dot1x default</code>	<code>enable authentication</code>	<code>password (User EXEC)</code>
<code>aaa authentication enable</code>	<code>enable password</code>	<code>show aaa ias-users</code>
<code>aaa authentication login</code>	<code>ip http authentication</code>	<code>show authentication methods</code>

aaa authorization network default radius	ip https authentication	show users accounts
aaa ias-user username	login authentication	show users login-history
aaa new-model	password (aaa IAS User Configuration)	username
clear (IAS)	password (Line Configuration)	–

aaa authentication dot1x default

Use the **aaa authentication dot1x default** command in Global Configuration mode to specify an authentication method for 802.1x clients. Use the **no** form of the command to return the authentication method to its default settings.

aaa authentication dot1x default does not support the **local** method. This is true for all switches using the 4.1.x.x or later firmware.

Syntax

aaa authentication dot1x default {radius | ias | local | none}

no aaa authentication dot1x default

Parameter Description

Parameter	Description
radius	Uses the list of all authentication servers for authentication.
ias	Uses the internal authentication server. Only EAP-MD5 authentication is supported for the internal authentication server.
local	Use the local authentication method.
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 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 privilege levels. 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:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The default enable list is **enableList**. It is used by console, telnet, and SSH and only contains the method *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 user. Only the RADIUS or TACACS methods can return an error. 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 level one user if no authentication method is defined. A level one user must

authenticate to get to privileged EXEC mode. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.



NOTE: Requests sent by the switch to a RADIUS server include the username "\$enabx\$", where x is the requested privilege level. 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 sets authentication when 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 set the authentication method required for user at login. To return to the default configuration, 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 a user logs in.
- *list-name* — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-15 characters)
- *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.

Keyword	Source or destination
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

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 used only if the previous method returns an error, not if there is an authentication failure. Only the RADIUS or TACACS+ methods can return an error. 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.



NOTE: Auth-Type=Local doesn't 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.

Example

The following example configures authentication login.

```
console(config)# aaa authentication login default
radius local enable none
```


aaa authorization

Use the **aaa authorization** command to 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 delete an authorization list.

Syntax

```
aaa authorization {commands|exec|network} {default|list-name} method1  
[method2]
```

```
no aaa authorization {commands|exec|network} {default|list-name}
```

Parameter Description

Parameter	Description
Authorization specifier:	
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 of commands. Only the default list is supported.
default	The default list of methods for authorization services (dfltCmdAuthList and dfltExecAuthList). Only the radius method is supported.
list-name	Character string used to name the list of accounting methods. The list name can consist of any alphanumeric character up to 15 characters in length. Use quotes around the list name if embedded blanks are contained in the list name.
method (<i>method1/method2</i> . ..)	The following authorization methods are supported: <ul style="list-style-type: none">• local – Perform local authorization (do not perform authorization).• none – Do not perform authorization.• radius – Request authorization from the configured RADIUS servers.• tacacs – Request authorization from the configured TACACS+ servers.

Default Configuration

Authorization is not enabled by default. Only TACACS is supported for authorization. Setting a **none** method for authorization authorizes all commands.

The following default Authorization Methods List is present by default:

Default List Name	Description	Authorization Method
dfltCmdAuthList	Default Command List	None
dfltExecAuthList	Default EXEC list	None

Command Mode

Global Config mode

User Guidelines

A maximum of five authorization method lists may be created for command types.

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.

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.

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.

Method	Notes
Local	The local method is not supported for authorization. This method is equivalent to selecting the none method.
TACACS	Only TACACS is supported for command authorization.

None	Selecting the none method authorizes all commands.
Radius	The radius method is only valid for EXEC authorization. Command authorization with RADIUS will work if and only if the applied authentication method is also radius.

aaa authorization network default radius

Use the **aaa authorization network default radius** command in Global Configuration mode to enable the switch to accept 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.

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 config 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
```

Parameter Description

This command does not require a parameter description.

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. PowerConnect switches only support the new model command set.

Syntax

```
aaa new-model
```

Parameter Description

This command does not require a parameter description.

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.

```
(config)# aaa new-model
```

clear (IAS)

Use the **clear aaa ias-users** command in Privileged EXEC mode to delete all IAS users.

Syntax

```
clear aaa ias-users
```

Parameter Description

This command does not require a parameter description.

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
```

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 }
```

Parameter Description

Parameter	Description
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).

Parameter	Description
list_name	Character string used to name the list of authorization methods. The list name can consist of any printable character. 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(config)# line console
console(config-line)# enable authentication default
```

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).
- **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 4.x firmware emulates industry standard behavior for enable mode authentication over SSH and telnet. In 4.x, 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.

Example

The following example defines password "xxxxyyzzz" to control access to user and privilege levels.

```
console(config)# enable password xxxxyyzzz
```

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:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

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 https server users. To return to the default configuration, use the **no** form of this command.

Syntax

```
ip https authentication method1 [method2...]
```

no ip https authentication

Parameter Description

method1 [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

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 TACACS+ is used as the authentication method for HTTP/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
```

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
```

password (aaa IAS User Configuration)

Use the **password** command in aaa IAS User Configuration mode to configure a password for a 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
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

aaa IAS User Configuration

User Guidelines

This command has no user guidelines.

Example

```
console#configure
console(config)#aaa ias-user username client-1
console(Config-IAS-User)#password client123
console(Config-IAS-User)#no password
```

Example of adding a MAB Client to the Internal user database:

```
console#configure
console(config)#aaa ias-user username 1f3ccb1157
```

```
console(Config-IAS-User)#password 1f3ccb1157
console(Config-IAS-User)#exit
console(config)#
```

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](#) on page 1559.

Syntax

```
password password [encrypted]
```

```
no password
```

- *password* — Password for this level. (Range: 8- 64 characters)
- `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 "mcmxxyy" on a line.

```
console(config-line)# password mcmxxyy
```

password (User EXEC)

Use the `password` command in User EXEC mode to allow a currently logged in user to change the password for only that user 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.



NOTE: For commands that configure password properties, see [Password Management Commands](#).

Syntax

```
password
```

Parameter Description

This command does not require a parameter description.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

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 in Privileged EXEC mode to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Syntax

```
show aaa ias-users [username]
```

Parameter Description

This command does not require a parameter description.

Default Behavior

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show aaa ias-users
```

```
UserName
```

```
-----
```

```
Client-1
```

```
Client-2
```

Following are the IAS configuration commands shown in the output of the show running-config command. Passwords shown in the command output are always encrypted.

```
aaa ias-user username client-1
```



```
password
a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46
104918f2c encrypted
exit
```

show aaa statistics

Use the `show aaa statistics` command in Privileged EXEC mode to display accounting statistics.

Syntax

```
show aaa statistics
```

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

```
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 authentication methods

Use the `show authentication methods` command in Privileged EXEC mode to display information about the authentication methods.

Syntax

```
show authentication methods
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 authorization methods

Use the `show authorization methods` command in Privileged EXEC mode to display the configured authorization method lists.

Syntax

```
show authorization methods
```

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Command authorization is supported only for the **line**, **telnet**, and **SSH** access methods.

Example

```
console#show authorization methods
```

Command Authorization List	Method	
dfltCmdAuthList	tacacs	none
list2	none	undefined
list4	tacacs	undefined

Line	Command Method List
Console	dfltCmdAuthList
Telnet	dfltCmdAuthList
SSH	dfltCmdAuthList

Exec Authorization List	Method	
dfltExecAuthList	tacacs	none
list2	none	undefined
list4	tacacs	undefined

Line	Exec Method List
Console	dfltExecAuthList
Telnet	dfltExecAuthList
SSH	dfltExecAuthList

show users accounts

Use the `show users accounts` command in Privileged EXEC mode to display the local user status with respect to user account lockout and password aging.

Syntax

`show users accounts`

Parameter Description

The following fields are displayed by this command.

Parameter	Description
User Name	Local user account's user name.
Privilege	User's access level (read only or read/write).
Lockout Status	Indicates whether the user account is locked out or not.
Password Expiration Date	Current password expiration date in date format.
Lockout	Displays the user's lockout status (True or False).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the local user database.

```
console#show users accounts
```

UserName	Privilege	Password	Password	Lockout
Aging	Expiry date			
admin	15	---	---	False
guest	15	---	---	False
brcml	1	---	---	False

```
console#show users accounts long
```

```
User Name
```

```
-----
```

```
asd
```

```
thisisaverylongusernameitisquitelong
```

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 [long]
```

- *name* — name of user. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example show 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

username

Use the **username** command in Global Configuration mode to add a new user to the local user 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} [privilege level|admin-profile profile] [encrypted]
```

```
no username name
```

Parameter Description

Parameter	Description
<i>name</i>	The name of the user. Range: 1-32 printable characters. The special characters allowed in the password include ! # \$ % & ' () * + , - . / : ; < = > @ [\] ^ _ ` { } ~. User names can contain blanks if the name is surrounded by double quotes.

Parameter	Description
<i>password</i>	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 ! # \$ % & ' () * + , - . / : ; < = > @ [\] ^ _ ` { } ~.
<i>level</i>	The user's privilege level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range: 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access.
<i>profile</i>	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

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.

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	No message is displayed.
Error Completion Message	Could not set user password!
Reason behind the failure	<p>1 Exceeds Minimum Length of a Password. Password should be in the range of 8-64 characters in length. Set minimum password length to 0 by using the <code>passwords min-length 0</code> command.</p> <p>2 Password should contain Minimum <number> uppercase-letters, <number> lowercase-letters, <number> numeric numbers, <number> special characters and <number> character classes and Maximum limit of <number> consecutive alphabetic and numeric characters. Maximum repetition of <number> alphabetic and number characters.</p> <p>3 Password should not contain the keywords <keyword1>, <keyword2> and <keyword3> in any form (reversed, substring or case-insensitive).</p>

Example

The following example configures user **bob** with password **xxxyymmmmm** 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 xxxyymmmmm
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 re-activate a locked user account.

Syntax

username *username* **unlock**

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Administrative Profiles Commands

Overview

The administrative profiles capability provides the network administrator control over which commands a user 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 PowerConnect 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 ..."
```



NOTE: If an "*" is used instead of an "=", the attribute is considered optional and devices which do not support this attribute will ignore it.

Commands in this Chapter

This chapter explains the following commands:

admin-profile	show admin-profiles
description (Administrative Profile Config)	show cli modes
rule	—

admin-profile

Use the **admin-profile** command in Global Config 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*

Parameter Description

Parameter	Description
profile-name	The name of the profile to create or delete. Range: 1 to 16 alphanumeric characters – may also include a hyphen.

Default Configuration

The administrative profiles are defined by default.

Command Mode

Global Config mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)#admin-profile qos
```

```
console(admin-profile)#
```

description (Administrative Profile Config)

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

Parameter Description

Parameter	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.

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
```

Parameter Description

Parameter	Description
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. Range: 1 to 128 characters). Regular expressions should conform to Henry Spencer's implementation of the POSIX 1003.2 specification. 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 in Privileged EXEC mode 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]`

Parameter Description

Parameter	Description
profile-name	The name of the administrative profile to display.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The following admin profiles are pre-defined 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.
```

```
-----  
Rule Perm      Type          Entity  
-----  
1 permit  command    access-list *  
2 permit  command    access-group *  
3 permit  mode       class-map
```

show cli modes

Use the `show cli modes` command in Privileged EXEC mode 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

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
```

ACL Commands

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 PowerConnect 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 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 physical 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 *hit*. Some hardware platforms have the ability to count the number of hits 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 PowerConnect ACL permit/deny rule specification supports a **log** parameter that enables hardware hit count collection and reporting. Depending on platform capabilities, logging can be specified for deny rules, permit rules, or both. 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. This is especially true in networks with protocols such as FCoE that have newly introduced Ether type values. 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 6-1 is a list of commonly used Ether types and, in Table 6-2 commonly used IP protocol numbers.

Table 6-1. Common Ethertypes

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

Table 6-2. Common IP Protocol Numbers

IP Protocol Numbers	Protocol
0x00	IPv6 Hop-by-hop option
0x01	ICMP
0x02	IGMP
0x06	TCP
0x08	EGP
0x09	IGP
0x11	UDP

Commands in this Chapter

This chapter explains the following commands:

<code>access-list</code>	<code>mac access-list extended rename</code>
<code>deny permit (IP ACL)</code>	<code>service-acl input</code>
<code>deny permit (Mac-Access-List-Configuration)</code>	<code>show service-acl interface</code>
<code>ip access-group</code>	<code>show ip access-lists</code>
<code>mac access-group</code>	<code>show mac access-list</code>
<code>mac access-list extended</code>	—

access-list

Use the `access-list` command in Global Configuration mode to create an Access Control List (ACL) that is identified by the parameter *list-name*.

The command specifies the queue identifier to which packets matching this rule are assigned. The command may also specify the mirror or redirect interface (unit/slot/port) to which packets matching this rule are copied or forwarded, respectively.

The time-range parameter 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.

```
access-list list-name {deny | permit} {every | {icmp | igmp | ip | tcp |  
udp | number} any} srcip srcmask[{eq {portkey | 0-65535}} dstip dstmask  
[{eq {portkey | 0-65535}} precedence precedence | tos tos tosmask | dscp  
dscp]} [log] [time-range time-range-name] [assign-queue queue-id] [{mirror  
| redirect} interface-id]
```

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

Parameter Description

Parameter	Description
<i>list-name</i>	Access-list name up to 31 characters in length.
deny permit	Specifies whether the IP ACL rule permits or denies an action.
every	Allows all protocols.
eq	Equal. Refers to the Layer 4 port number being used as match criteria. The first reference is source match criteria, the second is destination match criteria.
<i>number</i>	Standard protocol number. Protocol keywords icmp,igmp,ip,tcp,udp.
<i>srcip</i>	Source IP address.
<i>srcmask</i>	Source IP mask.
<i>dstip</i>	Destination IP address.
<i>dstmask</i>	Destination IP mask.
<i>portvalue</i>	The source layer 4 port match condition for the ACL rule is specified by the port value parameter (Range: 0–65535).
<i>portkey</i>	Or you can specify the <i>portkey</i> , which can be one of the following keywords: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
log	Specifies that this rule is to be logged.
<i>time-range-name</i>	Displays the name of the time-range if the ACL rule has referenced a time range.
assign-queue <i>queue-id</i>	Specifies the particular hardware queue for handling traffic that matches the rule. (Range: 0-6)
mirror <i>interface</i>	Allows the traffic matching this rule to be copied to the specified interface.
redirect <i>interface</i>	This parameter allows the traffic matching this rule to be forwarded to the specified unit/slot/port.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Access list names can consist of any printable character. Names can be up to 31 characters in length.

Examples

The following examples create an ACL to discard any HTTP traffic from 192.168.77.171, but allow all other traffic from 192.168.77.171:

```
console(config)#access-list alpha deny ip
192.168.77.171 0.0.0.0 0.0.0.0 255.255.255.255 eq
http
```

```
console(config)#access-list alpha permit ip
192.168.77.171 0.0.0.0 any
```

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.

The command is enhanced to accept 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.

Syntax

```
{deny | permit} {every | any} {dstmac | any} [ethertypekey | 0x0600-
0xFFFF] vlan {eq 0-4095} [cos 0-7] [[log] [time-range time-range-name]
[assign-queue queue-id] [{mirror | redirect} interface-id]
```



```
{deny | permit} {every | {{icmp | igmp | ip | tcp | udp | number} srcip
srcmask [{eq {portkey | 0-65535} dstip dstmask [{eq {portkey| 0-65535}]
[precedence precedence | tos tos tosmask | dscp dscp] [log] [time-range
time-range-name] [assign-queue queue-id] [{mirror | redirect} interface-id]
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

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 a port value should also specify the protocol and ethertype. Rules that specify a protocol should also specify the ethertype value for the frame. 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) and the ethertype field (0x800 – IPv4). Below is a list of commonly used etherypes:

Ethertype	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on LAN Packet
0x8035	Reverse Address Resolution Protocol (RARP)
0x8100	VLAN tagged frame (IEEE 802.1Q)
0x86DD	Internet Protocol version 6 (IPv6)
0x8808	MAC Control

Ethertype	Protocol
0x8809	Slow Protocols (IEEE 802.3)
0x8870	Jumbo frames
0x888E	EAP over LAN (EAPOL – 802.1x)
0x88CC	Link Layer Discovery Protocol
0x8906	Fibre Channel over Ethernet
0x8914	FCoE Initialization Protocol
0x9100	Q in Q

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.

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.

Syntax

```
{deny | permit} {{any | srcmac srcmacmask} {any | bpdu | dstmac
dstmacmask}} [ethertypekey | 0x0600-0xFFFF] vlan {eq 0-4095} [cos 0-7]
[[log] [time-range time-range-name] [assign-queue queue-id] [{mirror |
redirect} interface-id]
```

Parameter Description

Parameter	Description
<i>srcmac</i>	Valid source MAC address in format xxxx.xxxx.xxxx.
<i>srcmacmask</i>	Valid MAC address bitmask for the source MAC address in format xxxx.xxxx.xxxx.
<i>any</i>	Packets sent to or received from any MAC address
<i>dstmac</i>	Valid destination MAC address in format xxxx.xxxx.xxxx.
<i>dstmacmask</i>	Valid MAC address bitmask for the destination MAC address in format xxxx.xxxx.xxxx.
<i>bpdu</i>	Bridge protocol data unit
<i>ethertypekey</i>	Either a keyword or valid four-digit hexadecimal number. (Range: Supported values are appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmlcast, mplsucast, Netbios, novell, pppoe, rarp.)
<i>0x0600-0xFFFF</i>	Specify custom ethertype value (hexadecimal range 0x0600-0xFFFF).
<i>vlan eq</i>	VLAN number. (Range 0-4095)
<i>cos</i>	Class of service. (Range 0-7)
<i>log</i>	Specifies that this rule is to be logged.
<i>time-range-name</i>	Use the time-range parameter to impose a time limitation on the MAC ACL rule as defined by the parameter <i>time-range-name</i> .
<i>assign-queue</i>	Specifies particular hardware queue for handling traffic that matches the rule.
<i>queue-id</i>	0-6, where n is number of user configurable queues available for that hardware platform.
<i>mirror</i>	Copies the traffic matching this rule to the specified interface.
<i>redirect</i>	Forwards traffic matching this rule to the specified physical interface.
<i>interface</i>	Valid physical interface in <i>unit/slot/port</i> format, for example 1/0/12.

Default Configuration

This command has no default configuration.

Command Mode

Mac-Access-List Configuration mode

User Guidelines

The **no** form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather the entire ACL must be deleted and respecified.

The `assign-queue` and `redirect` parameters are only valid for `permit` commands.

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)#deny 0806.c200.0000
ffff.ffff.ffff any
```

ip access-group

Use the `ip access-group` command in Global and Interface Configuration modes to apply an IP based egress ACL on an Ethernet interface or a group of interfaces. An IP based ACL should have been created by the `access-list name ...` command with the same name specified in this command.

Use the `no ip access-group` command to disable an IP based egress ACL on an Ethernet interface or a group of interfaces.

Syntax

```
ip access-group name [direction] [seqnum]
```

```
no ip access-group name direction seqnum
```

- *name* — Access list name. (Range: Valid IP access-list name up to 31 characters in length)

- *direction* — Direction of the ACL. (Range: **in** or **out**. Default is *in*.)
- *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

Global mode command configures the ACL on all the interfaces, whereas the interface mode command does so for the interface.

Examples

```
console(config)#ip access-group aclname in
console(config)#no ip access-group aclname in
console(config)#ip access-group aclname1 out
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#ip access-group aclname
out 2
console(config-if-Te1/0/1)#no ip access-group aclname
out
```

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 in the in-bound direction.

Syntax

```
mac access-group name [direction] [sequence]
```

no mac access-group *name*

- *name* — Name of the existing MAC access list. (Range: 1-31 characters)
- *direction* — Only the in-bound direction is supported.
- *sequence* — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1-4294967295)

Default Configuration

The default direction is **in** (in-bound).

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, VLAN or Port Channel) mode

User Guidelines

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.

This command specified in Interface Configuration mode only affects a single interface.

Example

The following example assigns a MAC access group to port 1/0/1 with the name DELL123.

```
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#mac access-group DELL123
```

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.

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 LVL7DELL
console(config-mac-access-list)#
```

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 rename DELL1  
DELL2
```

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 |  
blocksstp | blockall}
```

```
no service-acl input
```

Parameter Description

Parameter	Description
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.
blocksstp	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

This command has no default configuration.

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 can only be entered once per interface if no intervening **no service-acl input** command has been entered.

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}
```

Parameter Description

Parameter	Description
interface-id	Any physical or logical interface. See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show service-acl interface gi1/0/1
```

```
Block CDP..... Enable
Block VTP.....Enable
Block DTP.....Enable
Block UDLD..... Enable
Block PAGP.....Enable
Block SSTP..... Enable
Block All..... Enable
```

show ip access-lists

Use the `show ip access-lists` command in Privileged EXEC mode to display an IP ACL and time-range parameters.

Syntax

```
show ip access-lists [accesslistnumber]
```

Parameter Description

Parameter	Description
<i>accesslistnumber</i>	The number used to identify the IP ACL.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays IP ACLs configured on a device.

```
console#show ip access-lists
```

```
Current number of ACLs: 2 Maximum number of ACLs: 100
```

ACL Name Vlan (s)	Rules	Interface (s)

ACL40	1	
ACL41	1	

show mac access-list

Use the `show mac access-list` command in Privileged EXEC mode to display a MAC access list and all of 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-list name
```

Parameter Description

Parameter	Description
<i>Name</i>	Use the <i>name</i> parameter to identify a specific MAC ACL to display.

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a MAC access list and all associated rules.

```
console#show mac access-list DELL123
```

The command output provides the following information:

Fields	Description
MAC ACL Name	The name of the MAC access list.
Rules	The number of user-configured rules defined for the MAC ACL. The implicit 'deny all' rule defined at the end of every MAC ACL is not included.
Interfaces	Displays the list of interfaces (unit/slot/port) to which the MAC ACL is attached in a given direction.

Address Table Commands

Static MAC Filtering allows the administrator to add a number of unicast or multicast MAC addresses directly to the forwarding database. This is typically a small number relative to the total size of the database. Associated with each static MAC address is a set of source ports, a set of destination ports and VLAN information.

Any packet with a particular static MAC address in a particular VLAN is admitted only if the ingress port is in the set of source ports; otherwise, the packet is dropped. On the egress side, the packet, if admitted, is sent out of all the ports that are in the set of destination ports.

Upon ingress, each packet's destination MAC address is compared against the forwarding database. If the address is not in the table, the packet is flooded to all other ports in the VLAN. If the address is in the table, then it is checked to see if it has been defined as a filter. If the MAC address is not defined as a filter, then the packet is forwarded.

If the specific destination MAC address is defined as a filter, then the ingress port number is compared to the set of source ports listed for the address. If the port of ingress is not in the set of source ports, then the packet is immediately discarded. If the ingress port is a member of the set of source ports, then the packet is admitted.

For packets admitted because of a MAC filter match only, the following additional steps are performed. Note that all other egress processing remains unchanged. At the egress port, if the destination port number is in the set of destination ports, the packet is forwarded. If the destination port is not in the set of destination ports, then the packet is discarded.

Static entries are never aged and can only be removed by user command.

Commands in this Chapter

This chapter explains the following commands:

<code>clear mac address-table</code>	<code>mac address-table static</code>	<code>show mac address-table count</code>
<code>mac address-table aging-time</code>	<code>port security</code>	<code>show mac address-table dynamic</code>
<code>mac address-table multicast filtering</code>	<code>port security max</code>	<code>show mac address-table interface</code>
<code>mac address-table multicast forbidden address</code>	<code>show mac address-table multicast</code>	<code>show mac address-table static</code>
<code>mac address-table multicast forbidden forward-unregistered</code>	<code>show mac address-table filtering</code>	<code>show mac address-table vlan</code>
<code>mac address-table multicast forward-all</code>	<code>show mac address-table</code>	<code>show ports security</code>
<code>mac address-table multicast forward-unregistered</code>	<code>show mac address-table address</code>	<code>show ports security addresses</code>
<code>mac address-table multicast static</code>	<code>show mac address-table count</code>	

clear mac address-table

Use the `clear mac address-table` command in Privileged EXEC mode to remove learned entries from the forwarding database.

Syntax

```
clear mac address-table dynamic [address mac-addr | interface interface-id | vlan vlan-id]
```

Parameter Description

Parameter	Description
<code>mac-addr</code>	Delete the specified MAC address.

Parameter	Description
<i>interface-id</i>	Delete all dynamic MAC addresses on the specified physical port or port channel.
<i>vlan-id</i>	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
```

Parameter Description

Parameter	Description
0	Disable aging time for the MAC Address Table

Parameter	Description
<i>10-1000000</i>	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 filtering

Use the `mac address-table multicast filtering` command in Global Configuration mode to enable filtering of Multicast addresses. To disable filtering of Multicast addresses, use the `no` form of the command.

Syntax

`mac address-table multicast filtering`

`no mac address-table multicast filtering`

Parameter Description

This command has no arguments or keywords.

Default Configuration

Multicast filtering is disabled by default. The switch will flood multicast packets to all ports belonging to the received VLAN and ignores the settings of the `mac address-table multicast forbidden` and `mac address-table multicast forward-unregistered` commands.

Command Mode

Global Configuration mode

User Guidelines

If switches exist on the VLAN, and IGMP snooping is not enabled, use the `mac address-table multicast forward-all` command to enable forwarding all Multicast packets to the Multicast routers.

Example

In this example, multicast filtering is enabled and multicast frames will behave according to the setting of the `mac address-table multicast forward-unregistered` and `mac address-table multicast forbidden forward-unregistereed` command settings.

```
console(config)#mac address-table multicast filtering
```

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 return to the system default, use the `no` form of this command. If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.

Syntax

```
mac address-table multicast forbidden address vlan vlan-id {mac-multicast-address | ip-multicast-address} {add | remove} interface {gigabitethernet | port-channel | tengigabitethernet | fortygigabitethernet} interface-list  
no mac address-table multicast forbidden address vlan vlan-id {mac-multicast-address | ip-multicast-address}
```

Parameter Description

Parameter	Description
<code>add</code>	Adds ports to the group. If no option is specified, this is the default option.
<code>remove</code>	Removes ports from the group.
<code>vlan vlan-id</code>	A valid vlan-id. (Range 1-4093)
<code>mac-multicast-address</code>	MAC Multicast address in the format xxxx.xxxx.xxxx.
<code>ip-multicast-address</code>	IP Multicast address.
<code>interface-list</code>	Specify a comma separated list of interfaces, a range of interfaces, or a combination of both. Interfaces can be port-channel numbers or physical ports in unit/slot/port format.

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.

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 gigabitethernet
2/0/9
```

mac address-table multicast forbidden forward-unregistered

Use the `mac address-table multicast forbidden forward-unregistered` command in Global Configuration mode to forbid forwarding unregistered-multicast-addresses. Use the `no` form of this command to return to the default.

Syntax

`mac address-table multicast forbidden forward-unregistered vlan vlan-id`

`no mac address-table multicast forbidden forward-unregistered vlan vlan-id`

Parameter Description

Parameter	Description
<code>vlan <i>vlan-id</i></code>	Valid VLAN ID (Range 1-4093).

Default Configuration

The default for this command is *not forbidden*.

Command Mode

Global configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example forbids forwarding unregistered multicast addresses on VLAN8.

```
console(config)#mac address-table multicast forbidden  
forward-unregistered vlan 8
```

mac address-table multicast forward-all

Use the `mac address-table multicast forward-all` command in Interface Configuration mode to enable forwarding of all Multicast packets. To restore the default, use the `no` form of the `mac address-table multicast forward-all` command.

Syntax

`mac address-table multicast forward-all vlan vlan-id`

`no mac address-table multicast forward-all vlan vlan-id`

Parameter Description

Parameter	Description
<code>vlan <i>vlan-id</i></code>	A valid VLAN ID (Range 1-4093).

Default Configuration

Forward-unregistered.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In this example, all VLAN1 Multicast packets are forwarded.

```
console(config)#mac address-table multicast forward-  
all vlan 1
```

mac address-table multicast forward-unregistered

Use the `mac address-table multicast forward-unregistered` command in Global Configuration mode to enable the forwarding of unregistered multicast addresses.

Syntax

`mac address-table multicast forward-unregistered vlan vlan-id`

Parameter Description

Parameter	Description
<code>vlan <i>vlan-id</i></code>	A valid VLAN ID (Range 1-4093).

Default Configuration

Forward-unregistered

Command Mode

Global Configuration mode

User Guidelines

If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.



NOTE: Do not use the `mac address-table multicast forbidden forward-unregistered` command with the `mac address-table multicast forward-unregistered` command on the same interface.

Example

The following example displays how to enable forwarding of unregistered multicast addresses.

```
console(config)#bridge multicast forward-unregistered  
vlan 1
```

mac address-table multicast static

Use the `mac address-table multicast static` command in Global Configuration mode to register MAC layer Multicast addresses to the bridge table and to add ports to the group statically. To deregister the MAC address, use the `no` form of the `mac address-table multicast static` command.

Syntax

```
mac address-table multicast static vlan vlan-id {mac-multicast-address | ip-multicast-address} [add | remove] [interface {gigabitethernet | port-channel | tengigabitethernet | fortygigabitethernet} interface-list]
```

```
no mac address-table multicast static vlan
```

Parameter Description

Parameter	Description
add	Adds ports to the group. If no option is specified, this is the default option.
remove	Removes ports from the group.
vlan <i>vlan-id</i>	Valid vlan ID (1-4093).
<i>mac-multicast-address</i>	MAC multicast address in the format xxxx.xxxx.xxxx.
<i>ip-multicast-address</i>	IP multicast address.
interface <i>interface-list</i>	Specify a comma separated list of interfaces, a range of interfaces, or a combination of both. Interfaces can be port-channel numbers or physical ports in unit/slot/port format.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

If the command is executed without **add** or **remove**, the command registers only the group in the bridge database.

Static Multicast addresses can be defined only on static VLANs.

Examples

The following example registers the MAC address.

```
console(config)#mac address-table vlan 8 multicast
static 0100.5e02.0203
```

The following example registers the MAC address and adds ports statically.

```
console(config)#interface vlan 8
console(config)# mac address-table vlan 8 multicast
static 0100.5e02.0203 add interface gigabitethernet
1/0/1-9, 1/0/2
```

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 {gigabitethernet |
port-channel | tengigabitethernet | fortygigabitethernet} interface-id
no mac address-table static mac-addr vlan vlan-id [interface
{gigabitethernet | port-channel | tengigabitethernet |
fortygigabitethernet} interface-id]
```

Syntax Description

Parameter	Description
<i>mac-address</i>	A valid MAC address in the format xxxx.xxxx.xxxx.
<i>vlan-id</i>	Valid VLAN ID (1-4093)
<i>interface-id</i>	A valid physical unit/slot/port or port-channel number.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 to the MAC address table.

```
console(config)# mac address-table static
3AA2.64B3.A245 vlan 1 interface gigabitethernet 1/0/8
```

port security

Use the **port security** command in Interface Configuration mode to disable the learning of new addresses on an interface. To enable new address learning, use the **no** form of the **port security** command.

Syntax

```
port security [discard]
```

```
no port security
```

- **discard** — Discards frames with unlearned source addresses. This is the default if no option is indicated.

Default Configuration

Disabled—No port security

Command Mode

Interface Configuration (*gigabitethernet*, *port-channel*, *tengigabitethernet*, *fortygigabitethernet*) mode

User Guidelines

When port security is enabled on an interface, all dynamic entries learned up to that point are flushed, and new entries can be learned only to the limit set by the **port security max** command. The default limit is 100 dynamic MAC addresses.

Example

In this example, frame forwarding is enabled without learning, and with traps sent every 100 seconds on port gi1/0/1.

```
console(config)#interface gigabitethernet te1/0/1
console(config-if-Te1/0/1)#port security trap 100
```

port security max

Use the **port security max** command in Interface Configuration mode to configure the maximum addresses that can be learned on the port while the port is in port security mode. To return to the system default, use the **no** form of this command.

Syntax

```
port security max max-addr
```

```
no port security max
```

- *max-addr* — The maximum number of addresses that can be learning on the port. (Range: 0-600)

Default Configuration

The default value for this command is 100.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows using this command in Ethernet Interface Configuration mode.

```
console(config-if-Te1/0/3)# port security max 80
```

show mac address-table multicast

Use the `show mac address-table multicast` command in Privileged EXEC mode to display Multicast MAC address table information.

Syntax

```
show mac address-table multicast [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 format. Can be *ip* or *mac*.

Default Configuration

If format is unspecified, the default is *mac*.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

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.

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.

show mac address-table filtering

Use the `show mac address-table filtering` command in Privileged EXEC mode to display the Multicast filtering configuration.

Syntax

```
show mac address-table filtering vlan-id
```

- *vlan_id* — A valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

In this example, the Multicast configuration for VLAN 1 is displayed.

```
console#show mac address-table filtering 1
```

Filtering: Enabled

VLAN: 1

Mode:

Forward-Unregistered

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
```

Parameter Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```

```

Vlan Mac Address      Type      Port
-----
0 001E.C9AA.AE19 Management CPU Interface: 0/5/
1 001E.C9AA.AC19 Dynamic   Gi1/0/21
1 001E.C9AA.AE1B Management V11
10 001E.C9AA.AE1B Management V110
90 001E.C9AA.AE1B Management V190

```

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]
```

Parameter Description

Parameter	Description
mac-address	A MAC address with the format xxxx.xxxx.xxxx.
interface-id	Display information for a specific interface. Valid interfaces include physical 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, Config mode and all Config sub-modes

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
```

```
Vlan Mac Address      Type      Port
-----
1      0000.E26D.2C2A Dynamic  1/0/1
```

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]
```

Parameter Description

Parameter	Description
<i>interface-id</i>	Specify an interface type; valid interfaces include physical ports and port channels.
<i>vlan-id</i>	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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the addresses in the Forwarding Database:

```
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]
```

Parameter Description

Parameter	Description
mac-address	A MAC address with the format xxxx.xxxx.xxxx.
interface-id	Display information for a specific interface. Valid interfaces include physical 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

In this example, all dynamic entries in the mac address-table are displayed.

```
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]
```


Parameter Description

Parameter	Description
interface-id	Specify an interface type. Valid interfaces include physical 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, Config mode and all Config sub-modes

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]
```

Parameter Description

Parameter	Description
mac-address	A MAC address with the format xxxx.xxxx.xxxx.
interface-id	Specify an interface type; valid interfaces include physical 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, Config mode and all Config sub-modes

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
```

```
Vlan Mac Address      Type      Port  
---- -
```

```
1      0001.0001.0001 Static    gi1/0/1
```

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]
```

Parameter Description

Parameter	Description
<i>vlan-id</i>	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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
console#show mac address-table vlan 1
```

```
Mac Address Table
```

```
-----  
Vlan  Mac Address      Type    Ports  
-----  
-----
```

```
1 0000.0001.0000 Dynamic gil/0/1
1 0000.8420.5010 Dynamic gil/0/1
1 0000.E26D.2C2A Dynamic gil/0/1
1 0000.E89A.596E Dynamic gil/0/1
1 0001.02F1.0B33 Dynamic gil/0/1
```

Total Mac Addresses for this criterion: 5

show ports security

Use the `show ports security` command in Privileged EXEC mode to display the port-lock status.

Syntax

```
show ports security [{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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

In this example, all classes of entries in the port-lock status are displayed.

```
console#show ports security
```

Port	Status	Action	Maximum	Trap	Frequency
----	-----	-----	-----	-----	-----

```

1/0/1 Locked Discard 3 Enable 100
1/0/2 Unlocked - 28 - -
1/0/3 Locked Discard, Shutdown 8 Disable -

```

The following table describes the fields in this example.

Field	Description
Port	The port number.
Status	The status can be one of the following: Locked or Unlocked.
Actions	Action on violations.
Maximum	The maximum addresses that can be associated on this port in Static Learning mode or in Dynamic Learning mode.
Trap	Indicates if traps would be sent in case of violation.
Frequency	The minimum time between consecutive traps.

show ports security addresses

Use the `show ports security addresses` command in Privileged EXEC mode to display current dynamic addresses in locked ports.

Syntax

```

show ports security addresses {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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following example displays dynamic addresses for port channel number 1/0/1.

```
console#show ports security addresses Te1/0/1
```

```
Dynamic addresses: 83
```

```
Maximum addresses: 100
```

```
Learned addresses
```

```
-----
```

Auto-VoIP Commands

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 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.

Commands in this Chapter

This chapter explains the following commands:

[show switchport voice](#)

[switchport voice detect auto](#)

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 [gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port / fortygigabitethernet unit/slot/port]
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Examples

The following example shows command output when a port is not specified:

```
console#show switchport voice
```

Interface	Auto VoIP Mode	Traffic Class
Gi1/0/1	Disabled	6
Gi1/0/2	Disabled	6
Gi1/0/3	Disabled	6
Gi1/0/4	Disabled	6
Gi1/0/5	Disabled	6
Gi1/0/6	Disabled	6

Gi1/0/7	Disabled	6
Gi1/0/8	Disabled	6
Gi1/0/9	Disabled	6
Gi1/0/10	Disabled	6
Gi1/0/11	Disabled	6
Gi1/0/12	Disabled	6
Gi1/0/13	Disabled	6
Gi1/0/14	Disabled	6
Gi1/0/15	Disabled	6
Gi1/0/16	Disabled	6
Gi1/0/17	Disabled	6
Gi1/0/18	Disabled	6
Gi1/0/19	Disabled	6
Gi1/0/20	Disabled	6
Gi1/0/21	Disabled	6
Gi1/0/22	Disabled	6
Gi1/0/23	Disabled	6
Gi1/0/24	Disabled	6
Po1	Disabled	6
Po2	Disabled	6
Po3	Disabled	6
Po4	Disabled	6
Po5	Disabled	6
Po6	Disabled	6
Po7	Disabled	6
Po8	Disabled	6

Po9	Disabled	6
Po10	Disabled	6
Po11	Disabled	6
Po12	Disabled	6
Po13	Disabled	6
Po14	Disabled	6
Po15	Disabled	6

--More-- or (q)uit

The following example shows command output when a port is specified:

```
console#show switchport voice gigabitethernet 1/0/1
```

Interface	Auto VoIP Mode	Traffic Class
-----	-----	-----
Gi1/0/1	Disabled	6

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, Config mode and all Config sub-modes,
Interface (gigabitethernet, port-channel, tengigabitethernet,
fortygigabitethernet) Configuration mode

User Guidelines

This command has no user guidelines

Example

```
console(config)#interface tengigabitethernet 1/0/1  
console(config-if-Te1/0/1)#switchport voice detect  
auto
```


CDP Interoperability Commands

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. PowerConnect 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 Chapter

This chapter explains the following commands:

<code>clear isdp counters</code>	<code>show isdp</code>
<code>clear isdp table</code>	<code>show isdp entry</code>
<code>isdp advertise-v2</code>	<code>show isdp interface</code>
<code>isdp enable</code>	<code>show isdp neighbors</code>
<code>isdp holdtime</code>	<code>show isdp traffic</code>
<code>isdp timer</code>	—

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. Use 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 (Ethernet) configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example enables isdp on interface 1/0/1.

```
console(config)#interface gigabitethernet 1/0/1
console(config-if-Gi1/0/1)#isdp enable
```

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
```

Parameter Description

Parameter	Description
<i>time</i>	The time in seconds (range 10–255 seconds).

Default Configuration

The default holdtime is 180 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

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
```

Parameter Description

Parameter	Description
<i>time</i>	The time in seconds (range: 5–254 seconds).

Default Configuration

The default timer is 30 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

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, Config mode and all Config sub-modes

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..... QTFMPW82400020
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}
```

Parameter Description

Parameter	Description
all	Show ISDP settings for all devices.
<i>deviceid</i>	The device ID associated with a neighbor.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp entry Switch
```

```
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                               1/0/1
Port ID                                 GigabitEthernet1/1
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.
```

show isdp interface

The `show isdp interface` command displays ISDP settings for the specified interface.

Syntax

```
show isdp interface {all | gigabitethernet unit/slot/port | tengigabitethernet  
unit/slot/port | fortygigabitethernet unit/slot/port}
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp interface all
```

Interface	Mode
-----	-----
1/0/1	Enabled
1/0/2	Enabled
1/0/3	Enabled
1/0/4	Enabled
1/0/5	Enabled
1/0/6	Enabled
1/0/7	Enabled

```
1/0/8           Enabled
1/0/9           Enabled
1/0/10          Enabled
1/0/11          Enabled
1/0/12          Enabled
1/0/13          Enabled
1/0/14          Enabled
1/0/15          Enabled
1/0/16          Enabled
1/0/17          Enabled
1/0/18          Enabled
1/0/19          Enabled
1/0/20          Enabled
1/0/21          Enabled
1/0/22          Enabled
1/0/23          Enabled
1/0/24          Enabled
```

```
console#show isdp interface gigabitethernet 1/0/1
```

```
Interface      Mode
-----
1/0/1          Enabled
```

show isdp neighbors

The `show isdp neighbors` command displays the list of neighboring devices.

Syntax

```
show isdp neighbors {[gigabitethernet unit/slot/port | tengigabitethernet  
unit/slot/port | fortygigabitethernet | detail]}
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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, S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Hold	Cap.	Platform	Port ID
-----	----	-----	-----	-----	-----
Switch	1/0/1	165	RI	cisco WS-C4948	GigabitEthernet1/1

```
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                1/0/1
Port ID                  GigabitEthernet1/1
Holdtime                 162
Advertisement Version    2
Entry last changed time 0 days 00:55:20
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 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, Config mode and all Config sub-modes

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.....	4253
ISDPv2 Packets Transmitted.....	4351
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

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 PowerConnect DHCP Relay supports DHCP Relay Option 82 circuit-id and remote-id for a VLAN.

Commands in this Chapter

This chapter explains the following commands:

<code>dhcp l2relay</code> (Global Configuration)	<code>show dhcp l2relay stats interface</code>
<code>dhcp l2relay</code> (Interface Configuration)	<code>show dhcp l2relay subscription interface</code>
<code>dhcp l2relay circuit-id</code>	<code>show dhcp l2relay agent-option vlan</code>
<code>dhcp l2relay remote-id</code>	<code>show dhcp l2relay vlan</code>
<code>dhcp l2relay trust</code>	<code>show dhcp l2relay circuit-id vlan</code>
<code>dhcp l2relay vlan</code>	<code>show dhcp l2relay remote-id vlan</code>
<code>show dhcp l2relay all</code>	<code>clear dhcp l2relay statistics interface</code>
<code>show dhcp l2relay interface</code>	—

`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-range
```

```
no dhcp l2relay circuit-id vlan vlan-range
```

Parameter Description

Parameter	Description
<i>vlan-range</i>	The list of VLAN IDs.

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-range
```

```
no dhcp l2relay remote-id remoteId vlan vlan-range
```

Parameter Description

Parameter	Description
<i>remoteId</i>	The string to be used as the remote ID in the Option 82 (Range: 1 - 128 characters).

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-range
no dhcp l2relay vlan vlan-range
```

Parameter Description

Parameter	Description
vlan-range	The list of VLAN IDs.

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
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        broadcom
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 in Privileged EXEC mode to display DHCP L2 Relay configuration specific to interfaces.

Syntax

```
show dhcp l2relay interface {all | interface-id}
```

Parameter Description

Parameter	Description
all	Show all interfaces.
interface-id	A physical interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

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 in Privileged EXEC mode to display DHCP L2 Relay statistics specific to interfaces.

Syntax

```
show dhcp l2relay stats interface {all | interface-id}
```

Parameter Description

Parameter	Description
all	Show all interfaces.
interface-id	A physical interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show dhcp l2relay stats interface all
```

```
DHCP L2 Relay is Enabled.
```

```
Interface  UntrustedServer  UntrustedClient
TrustedServer      TrustedClient
                MsgsWithOpt82    MsgsWithOpt82
MsgsWithoutOpt82  MsgsWithoutOpt82
-----
-----
Gi1/0/1      0                    0                    0
0
Gi1/0/2      0                    0                    3
7
Gi1/0/3      0                    0                    0
0
```

show dhcp l2relay subscription interface

Use the `show dhcp l2relay subscription interface` command in Privileged EXEC mode to display DHCP L2 Relay Option-82 configuration specific to interfaces.

Syntax

```
show dhcp l2relay subscription interface {all | interface-id}
```

Parameter Description

Parameter	Description
all	Show all interfaces.
interface-id	A physical interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

show dhcp l2relay agent-option vlan

Use the `show dhcp l2relay agent-option vlan` command in Privileged EXEC mode to display DHCP L2 Relay Option-82 configuration specific to VLANs.

Syntax

`show dhcp l2relay agent-option vlan vlan-range`

Parameter Description

Parameter	Description
vlan-range	Show information for the specified VLAN range. A range may be a single VLAN ID or two VLAN IDs separated by a single dash with no embedded spaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display whether DHCP L2 Relay is globally enabled on the specified VLAN or VLAN range.

Syntax

```
show dhcp l2relay vlan vlan-range
```

Parameter Description

Parameter	Description
vlan-range	Show information for the specified VLAN range. A range may be a single VLAN ID or two VLAN IDs separated by a single dash with no embedded spaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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-range
```

Parameter Description

Parameter	Description
vlan-range	Show information for the specified VLAN range. A range may be a single VLAN ID or two VLAN IDs separated by a single dash with no embedded spaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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:

```
300
```

show dhcp l2relay remote-id vlan

Use the `show dhcp l2relay remote-id vlan` command in Privileged EXEC mode 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-range
```

Parameter Description

Parameter	Description
vlan-range	Show information for the specified VLAN range. A range may be a single VLAN ID or two VLAN IDs separated by a single dash with no embedded spaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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
```

```
-----
```

```
200remote_22
```

clear dhcp l2relay statistics interface

Use the `show dhcp l2relay statistics interface` command in Privileged EXEC mode 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}
```

Parameter Description

Parameter	Description
all	Show all interfaces.
interface-id	A physical 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 Management Interface Commands

PowerConnect 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 Chapter

This chapter explains the following commands:

[release dhcp](#)

[debug dhcp packet](#)

release dhcp

Use the `release dhcp` command in Privileged EXEC mode to force the DHCPv4 client to release a leased address.

Syntax

```
release dhcp interface-id
```

Parameter Description

Parameter	Description
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 Config)` command on page 511 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:

```
Interface does not have a DHCP-originated address.
```

The `release dhcp` option is applicable only for routing interfaces and not for 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 vlan2
```

renew dhcp

Use the `renew dhcp` command in Privileged EXEC mode to force the DHCP client to immediately renew an IPv4 address lease.

Syntax

```
renew dhcp {interface-id | out-of-band}
```

Parameter Description

Parameter	Description
interface-id	Any valid routing 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
```

Examples

The first example is for routing interfaces.

```
console#renew dhcp vlan 2
```

The second example is for out-of-band port.

```
console#renew dhcp out-of-band
```

debug dhcp packet

Use the `debug dhcp packet` command in Privileged EXEC mode 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

```
debug dhcp packet [transmit | receive]  
no debug dhcp packet [transmit | receive]
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

DHCP client already has packet tracing. This command turns the packet tracing on.

Example

The first example is for 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
```

show dhcp lease

Use the `show dhcp lease` command in Privileged EXEC mode to display IPv4 addresses leased from a DHCP server.

Syntax

```
show dhcp lease [interface interface-id]
```

Parameter Description

Parameter	Description
interface-id	Any valid IP interface (VLAN only). See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command lists all IPv4 addresses currently leased from a DHCP server on a routing interface. This command only applies to routing interfaces.

This command output provides the following information.

Term	Description
IP address, Subnet mask	The IP address and network mask leased from the DHCP server.
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface.

Term	Description
DHCP transaction id	The transaction ID of the DHCPv4 Client.
Lease	The time (in seconds) that the IP address was leased by the server.
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address.
Rebind	The time (in seconds) when the DHCP Rebind process starts.
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds.

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: 10.1.20.1 on interface VLAN10
```

```
Subnet mask: 255.255.255.0
```

```
    DHCP Lease server: 10.1.20.3, state: 5 Bound
```

```
    DHCP transaction id: 0x7AD
```

```
    Lease: 86400 secs, Renewal: 43200 secs,
    Rebind: 75600 secs
```

```
    Retry count: 0
```

```
IP address: 10.1.1.2 on interface VLAN20
```

```
Subnet mask: 255.255.255.0
```

```
    DHCP Lease server: 10.1.1.1, state: 5 Bound
```

```
    DHCP transaction id: 0x11EB
```

```
    Lease: 86400 secs, Renewal: 43200 secs,
    Rebind: 75600 secs
```

```
    Retry count: 0
```

```
console#show dhcp lease interface vl10
IP address: 10.1.20.1 on interface VLAN10
Subnet mask: 255.255.255.0
    DHCP Lease server: 10.1.20.3, state: 5 Bound
    DHCP transaction id: 0x7AD
    Lease: 86400 secs, Renewal: 43200 secs, Rebind:
75600 secs
    Retry count: 0
```


DHCP Snooping Commands

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 Chapter

This chapter explains the following commands:

<code>clear ip dhcp snooping binding</code>	<code>ip dhcp snooping trust</code>
<code>clear ip dhcp snooping statistics</code>	<code>ip dhcp snooping verify mac-address</code>
<code>ip dhcp snooping</code>	<code>show ip dhcp snooping</code>
<code>ip dhcp snooping binding</code>	<code>show ip dhcp snooping binding</code>
<code>ip dhcp snooping database</code>	<code>show ip dhcp snooping database</code>
<code>ip dhcp snooping database write-delay</code>	<code>show ip dhcp snooping interfaces</code>
<code>ip dhcp snooping limit</code>	<code>show ip dhcp snooping statistics</code>
<code>ip dhcp snooping log-invalid</code>	–

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 }
```

Syntax Description

Parameter	Description
*	Clear all DHCP Snooping entries.
interface-id	Clear all DHCP Snooping entries on the specified interface.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

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. Use the “no” form of this command to disable DHCP snooping.



NOTE: Effective with the June 2012 A02 release, the `ip dhcp snooping` command in Interface Configuration (VLAN) mode is deprecated in favor of the `ip dhcp snooping` command in Global Configuration mode.

Syntax

```
ip dhcp snooping
```

```
no ip dhcp snooping
```

Default Configuration

DHCP Snooping is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

In order to enable DHCP snooping, perform the following three steps:

- 1 Enable DHCP Snooping globally.
- 2 Enable DHCP Snooping per VLAN.
- 3 Set DHCP Snooping trusted port on the port in the DHCP server direction.

Example

The following configuration enables DHCP snooping on VLAN 1 for a switch connected to a DHCP server over interface *gi1/0/4*:

```
console(config)#ip dhcp snooping
console(config-if-vlan1)#ip dhcp snooping
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
{gigabitethernet unit/slot/port | tengigabitethernet unit/slot/port /
fortygigabitethernet unit/slot/port}
no ip dhcp snooping binding mac-address
```

Parameter Description

Parameter	Description
<i>mac-address</i>	The client's MAC address.
<i>vlan-id</i>	The number of the VLAN the client is authorized to use.
<i>ip-address</i>	The IP address of the client.
<i>interface</i>	The interface on which the client is authorized. The form is unit/slot/port.

Default Configuration

There are no static 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
1/0/1
```

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}
```

Parameter Description

Parameter	Description
<i>hostIP</i>	The IP address of the remote host.
<i>filename</i>	The name of the file for the database on the remote host. The filename may contain any printable character and is checked only when attempting to open the file.

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`

Parameter Description

Parameter	Description
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 control the maximum rate of DHCP messages. Use the `no` form of this command to reset the limit to the default.

Syntax

`ip dhcp snooping limit {none | rate rate [burst interval seconds]}`

`no ip dhcp snooping limit`

- *rate*—The maximum number of packets per second allowed (Range: 0–300 pps).
- *seconds*—The time allowed for a burst (Range: 1–15 seconds).

Default Configuration

DHCP snooping rate limiting is 15 packets per second.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

If DHCP packets are received on a port at a rate that exceeds the threshold for the specified time, the 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.

Use the **no shut** command to return a disabled port to service.

Examples

```
console(config-if-Gi1/0/1)#ip dhcp snooping limit  
none
```

```
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.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/0/1)#ip dhcp snooping log-invalid
```

```
console(config-if-1/0/1)#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

Interfaces connected to the DHCP server must be configured as trusted in order for DHCP snooping to operate.

Example

```
console(config-if-1/0/1)#ip dhcp snooping trust
console(config-if-1/0/1)#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 enabled 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
```

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 mode, Config mode and all Config sub-modes

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
```

Interface	Trusted	Log Invalid Pkts
-----	-----	-----
1/0/1	Yes	No
1/0/2	No	Yes
1/0/3	No	Yes
1/0/4	No	No
1/0/6	No	No

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]  
[vlan vlan-id]
```

- `static | dynamic`—Use these keywords to filter by static or dynamic bindings.
- `interface-id`—The interface for which to show bindings.
- `vlan-id`—The number of the VLAN for which to show bindings.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

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
00:02:B3:06:60:80	210.1.1.3	10	1/0/1
86400			

```
00:0F:FE:00:13:04    210.1.1.4          10    1/0/1
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
```

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, Config mode and all Config sub-modes

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*]

- interface—A valid physical interface.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip dhcp snooping interfaces
```

Interface	Trust State	Rate Limit	Burst
Interval		(pps)	
(seconds)			
-----	-----	-----	-----

1	1/0/1	No	15
1	1/0/2	No	15
1	1/0/3	No	15

```
console#show ip dhcp snooping interfaces
gigabitethernet 1/0/15
```

Interface	Trust State	Rate Limit	Burst
Interval		(pps)	
(seconds)			
-----	-----	-----	-----

1	1/0/15	Yes	15

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
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed by this command:

Fields	Description
MAC Verify Failures	The number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client MAC address mismatch.
Client Ifc Mismatch	The number of DHCP release and Deny messages received on the different ports than previously learned.
DHCP Server Msgs	The number of DHCP server messages received on untrusted ports.

Example

```
console#show ip dhcp snooping statistics
```

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
-----	-----	-----	-----
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0
1/0/9	0	0	0
1/0/10	0	0	0
1/0/11	0	0	0
1/0/12	0	0	0
1/0/13	0	0	0
1/0/14	0	0	0

1/0/15	0	0	0
1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0

Dynamic ARP Inspection

Commands

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 miscreant 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 Chapter

This chapter explains the following commands:

<code>arp access-list</code>	<code>ip arp inspection vlan</code>
<code>clear ip arp inspection statistics</code>	<code>permit ip host mac host</code>
<code>ip arp inspection filter</code>	<code>show arp access-list</code>
<code>ip arp inspection limit</code>	<code>show ip arp inspection</code>
<code>ip arp inspection trust</code>	<code>show ip arp inspection vlan</code>
<code>ip arp inspection validate</code>	—

arp 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 access-list acl-name`

`no arp 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 in Privileged EXEC mode to reset the statistics for Dynamic Address Resolution Protocol (ARP) inspection on all VLANs.

Syntax

```
clear ip arp inspection statistics
```

Parameter Description

This command does not require a parameter description.

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 the ARP ACL to be used for a single VLAN or a range of VLANs to filter invalid ARP packets. If the `static` keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. Use the “no” form of this command to unconfigure the ARP ACL.

Syntax

```
ip arp inspection filter acl-name vlan vlan-range [static]
```

```
no ip arp inspection filter acl-name vlan vlan-range [static]
```

- *acl-name*—The name of a valid ARP ACL. (Range: 1–31 characters)
- *vlan-range*—A valid VLAN range.

Default Configuration

No ARP ACL is configured.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

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-1/0/1)#ip arp inspection limit none
console(config-if-1/0/1)#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

There are no user guidelines for this command.

Example

```
console(config-if-1/0/3)#ip arp inspection trust
```

ip arp inspection validate

Use the `ip arp inspection validate` command to enable additional validation checks like source MAC address validation, destination MAC address validation or IP address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables source MAC address and destination MAC address validations and a second command enables IP address validation only, the source MAC address and destination MAC address validations are disabled as a result of the second command. Use the “no” form of this command to disable additional validation checks.

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

There are no user guidelines for this command

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-range [logging]
```

```
no ip arp inspection vlan vlan-range [logging]
```

- *vlan-range* — A valid range of VLAN IDs.

- **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

There are no user guidelines for this command.

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 a rule for a valid IP address and MAC address combination used in ARP packet validation. Use the “no” form of this command to delete an 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display the Dynamic ARP Inspection and status.

Syntax

```
show ip arp inspection [interfaces [interface-id] | statistics [vlan vlan-range]  
| vlan vlan-range]
```

Parameter Description

Parameter	Description
interfaces [<i>interface-id</i>]	Display the Dynamic ARP Inspection configuration on all the DAI enabled interfaces. Giving an interface argument, it displays the values for that interface.
statistics [vlan <i>vlan-range</i>]	Display the statistics of the ARP packets processed by Dynamic ARP Inspection. Given <i>vlan-range</i> 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 <i>vlan-range</i>	Display the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range. It also displays the global configuration values for source MAC validation, destination MAC validation and invalid IP validation.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The following information is displayed for each VLAN when a VLAN range is supplied:

Field	Description
VLAN	The VLAN-ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of invalid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP Snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example

Following is an example of the `show ip arp inspection` command.

```
console#show ip arp inspection
```

```
Source MAC Validation..... Disabled
```

```
Destination MAC Validation..... Disabled
```

```
IP Address Validation..... Disabled
```

```
VLANConfigurationLog InvalidACL NameStatic flag
```

```
-----
```

```
1 Disabled Enabled
```

```
console#
```

Following is an example of the `show ip arp inspection interfaces` command.

```
console#show ip arp inspection interfaces
```

Interface Interval	Trust State	Rate Limit (pps)	Burst (seconds)
-----	-----	-----	-----
1/0/1 1	Untrusted	15	
1/0/2 10	Untrusted	10	

Following is an example of the `show ip arp inspection statistics` command.

```
console#show ip arp inspection statistics
```

VLAN	Forwarded	Dropped
----	-----	-----
10	90	14
20	10	3

```
console#show ip arp inspection statistics vlan 10,20
```

VLAN	DHCP	ACL	DHCP	ACL	Bad
Src	Bad Dest	Invalid			
MAC	Drops	Drops	Permits	Permits	MAC
	IP				

```

-----
-----
10          11          1          65          25
1           1           0
20          1           0          8           2
0           1           1

```

show ip arp inspection vlan

Use the `show ip arp inspection vlan` command to display the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range. It also displays the global configuration values for source MAC validation, destination MAC validation and invalid IP validation.

Syntax

```
show ip arp inspection vlan [vlan-range]
```

Parameter Description

Parameter	Description
vlan-range	A valid VLAN range.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The following global parameters are displayed:

Parameter	Description
Source Mac Validation	If Source Mac validation of ARP frame is enabled.

Destination Mac Validation	If Destination Mac validation of ARP Response frame is enabled.
IP Address Validation	If IP address validation of ARP frame is enabled.

The following fields are displayed for each VLAN:

Field	Description
VLAN	The VLAN-ID for each displayed row.
Configuration	Whether DAI is enabled on the VLAN.
Log Invalid	Whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	ARP ACL Name if configured on the VLAN.
Static flag	If the ARP ACL is configured static on the VLAN.

Example

```
console#show ip arp inspection vlan 10-12
```

```
Source Mac Validation      : Disabled
```

```
Destination Mac Validation : Disabled
```

```
IP Address Validation      : Disabled
```

```

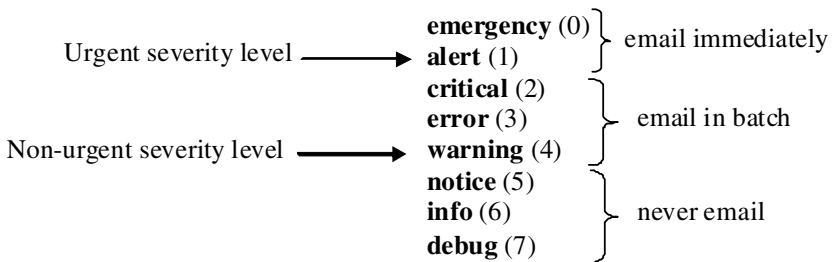
Vlan          Configuration      Log Invalid   ACL Name
Static flag
-----
 10          Enabled           Enabled      H2
Enabled
 11          Disabled          Enabled
 12          Enabled           Disabled

```


E-mail Alerting Commands

E-mail Alerting is an extension of the logging system. The PowerConnect 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 Chapter

This chapter explains the following commands:

logging email	show logging email statistics
logging email urgent	clear logging email statistics
logging traps	security
logging email message-type to-addr	mail-server ip-address hostname
logging email from-addr	port (Mail Server Configuration Mode)
logging email message-type subject	username (Mail Server Configuration Mode)
logging email logtime	password (Mail Server Configuration Mode)
logging email test message-type	show mail-server

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
```

Parameter Description

Parameter	Description
severity	<p>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.</p> <ul style="list-style-type: none">• 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

Parameter Description

Parameter	Description
severity	Log messages at or above this severity level are e-mailed immediately. 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. <ul style="list-style-type: none">• 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 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

Parameter Description

Parameter	Description
severity	<p>The severity level at which SNMP traps are logged. 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:</p> <ul style="list-style-type: none">• 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 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 now 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*

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command removes the configured **to-addr** field of e-mail.

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

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

There are no user guidelines for this command.

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

Parameter Description

This command does not require a parameter description.

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.

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

logging email logtime *time duration*

no logging email logtime

Parameter Description

Parameter	Description
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.

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`

Parameter Description

Parameter	Description
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.

show logging email statistics

Use the **show logging email statistics** command in Privileged EXEC mode to show the statistics about the e-mails. The command 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.

Syntax

show logging email statistics

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

clear logging email statistics

Use the **clear logging email statistics** command in Privileged EXEC mode to clear the e-mail alerting statistics.

Syntax

clear logging email statistics

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

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 {tls | none}
```

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is disabled.

Command Mode

Mail Server Configuration

User Guidelines

This command has no user guidelines.

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. The server address can be in the IPv4, IPv6, or DNS name format. Use the `no` form of this command to remove the configured SMTP server address.

Syntax

```
mail-server {ip-address ip-address | hostname hostname}
```

```
no mail-server {ip-address | hostname}
```

Parameter Description

Parameter	Description
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.

Field	Default
Email Alert Mail Server Port	25
Email Alert Security Protocol	none
Email Alert Username	admin
Email Alert Password	admin

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

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. Port can be set to 465 or 25. Use the **no** form of the command to revert the SMTP port to the default port.

Syntax

port *port*

no port

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is 25.

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. Messages are always sent in plain text mode.

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

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value for username is **admin**.

Command Mode

Mail Server Configuration

User Guidelines

This command has no user guidelines.

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

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value for password is **admin**.

Command Mode

Mail Server Configuration

User Guidelines

This command has no user guidelines.

show mail-server

Use the `show mail-server` command in Privileged EXEC mode to display the configuration of all the mail servers or a particular mail server.

Syntax

```
show mail-server {ip-address | hostname | all}
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show mail-server all
```

```
Mail Servers configuration:
```

```
No of mail servers configured:2
```

```
Mail Serqy ver1 configuration:
```

```
SMTP server IP Address:                10.131.1.11
```

```
SMTP server Port:                       465
```

```
SMTP server security protocol:         tls
```

SMTP server authentication details:

Username: admin

Mail server2 configuration:

SMTP server IP Address: 10.131.1.31

SMTP server Port: 465

SMTP server security protocol: tls

SMTP server authentication details:

Username: admin

console#show mail-server ip-address 10.131.1.11

SMTP server IP Address: 10.131.1.11

SMTP server Port: 465

SMTP server security protocol: tls

SMTP server authentication details:

Username: admin

Ethernet Configuration Commands

PowerConnect 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 PowerConnect 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. PowerConnect switching implements the flow control mechanism defined in IEEE 802.3 Annexes 31A and 31B (formerly IEEE 802.3x). PowerConnect switching is able to transmit a MAC Control frame containing the PAUSE opcode to halt transmission by the device receiving the PAUSE frame whenever internal congestion is detected by the switching fabric. 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` and `duplex` commands control interface link speeds and auto-negotiation. If either speed or duplex 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 and prefers full duplex over half duplex.

Commands in this Chapter

This chapter explains the following commands:

<code>clear counters</code>	<code>show interfaces configuration</code>	<code>speed</code>
<code>description</code>	<code>show interfaces counters</code>	<code>storm-control broadcast</code>
<code>duplex</code>	<code>show interfaces description</code>	<code>storm-control multicast</code>
<code>flowcontrol</code>	<code>show interfaces detail</code>	<code>storm-control unicast</code>
<code>interface</code>	<code>show statistics</code>	<code>switchport protected</code>
<code>interface range</code>	<code>show statistics switchport</code>	<code>switchport protected name</code>
<code>mtu</code>	<code>show storm-control</code>	<code>show switchport protected</code>
<code>show interfaces advertise</code>	<code>shutdown</code>	–

clear counters

Use the `clear counters` command in Privileged EXEC mode to clear statistics on an interface.

Syntax

```
clear counters [{gigabitethernet unit/slot/port | port-channel port-channel-
number | switchport | 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

In the following example, the counters for port 1/0/1 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-1/0/5)# description RD_SW#3
```

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
```

Parameter Description

Parameter	Description
auto	Auto negotiation is enabled for the port.
half	Force half-duplex operation.
full	Force full-duplex operation.

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 both the **speed** and **duplex** commands without using the **auto**

parameter. 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. Disabling auto-negotiation on 1G copper ports may lead to random frame loss as the clock master has not been arbitrated by the auto-negotiation process. Auto-negotiation is required on 10G/40G copper ports, and is recommended on all copper ports.

Example

The following example configures the duplex operation of gigabit Ethernet port 1/0/5 to force full duplex operation.

```
console(config)# interface gigabitethernet 1/0/5
console(config-if)# duplex full
```

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
no flowcontrol
```

Default Configuration

Flow Control is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In the following example, flow control is enabled.

```
console(config)# flowcontrol
```

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](#), [interface loopback](#), 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

It is possible to enter interface configuration mode from global configuration mode or from interface configuration mode.

Example

The following example enables gigabit port 2 on stack member 1 for configuration.

```
console(config)# interface gigabitethernet 1/0/2  
console (config-if)#
```

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 {port-range | port-type all}
```

Parameter	Description
<i>port-range</i>	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 Operating on Multiple Objects (Range) . The command line buffer parses up to the maximum number of command line characters possible in the <i>port-range</i> parameter.
<i>port-type</i>	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.

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
5/0/18-20,3/0/1-24
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,tengigabitEthernet 1/1/2
```

mtu

Use the **mtu** command in Interface Configuration mode to set the maximum transmission unit on an interface by adjusting the maximum size of received Ethernet frames. To return to the default setting, use the **no** form of this command.

Syntax

`mtu bytes`

`no mtu`

- *bytes* — Number of bytes (Range: 1518-9216)

Default Configuration

The default number of bytes is 1518 (1522 bytes of VLAN-tagged frames).

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Because the switch does not fragment frames, received frames that are larger than the MTU setting are dropped. Packets originated by the CPU are fragmented on transmission if the link MTU is smaller than the IP MTU. Setting the MTU less than the IPv4 MTU causes CPU-generated IPv4 packets to be fragmented. Setting the MTU less than the IPv6 MTU causes CPU-generated IPv6 packets to be dropped. Setting the MTU also automatically adjusts the IPv4 MTU. Port-channel and interface MTU settings are configured and maintained independently. Setting the MTU on a port-channel adjusts the operational MTU of an interface when the interface is a member of a LAG. The operational MTU is reset back to the interface MTU setting when the interface leaves the LAG.

Use the **show interfaces mtu** command to show the interface MTU.

Example

The following example of the `mtu` command increases maximum packet size to 9216 bytes.

```
console(config-if-1/0/5)#mtu 9216
```

show interfaces advertise

Use the `show interfaces advertise` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

```
Port  Type          Neg          Operational Link  
Advertisement
```

```
-----  
-----
```

```

1/0/2  1G-Copper  Enable  1000f, 100f, 100h, 10f, 10h
1/0/2  1G-Copper  Enable  1000f

```

Example #2

```

console# show interfaces advertise gigabitethernet
1/0/1

```

Port: Gigabitethernet 1/0/1

Type: 1G-Copper

Link state: Up

Auto negotiation: enabled

10h 10f 100h 100f 1000f

Admin Local Link -----

Advertisement	yes	yes	yes	yes	no
---------------	-----	-----	-----	-----	----

Example #3

```

console#show interfaces advertise gil/0/1

```

Port: Gil/0/1

Type: Gigabit - Level

Link State: Down

Auto Negotiation: Enabled

802.3az EEE: Disabled

Clock: Master

	1000f	1000h	100f	100h	10f	10h
--	-------	-------	------	------	-----	-----

Admin Local Link Advertisement	no	no	yes	no	yes	no
--------------------------------	----	----	-----	----	-----	----

Oper Local Link Advertisement	no	no	yes	no	yes	no
-------------------------------	----	----	-----	----	-----	----

Oper Peer Advertisement	no	no	yes	yes	yes	yes
-------------------------	----	----	-----	-----	-----	-----

Priority Resolution	-	-	yes	-	-	-
---------------------	---	---	-----	---	---	---

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, Config mode and all Config sub-modes

User Guidelines

This command has no use guidelines.

Example

The following example displays the configuration for all configured interfaces:

```
console>show interfaces configuration
```

Port	Type	Duplex	Speed	Neg	Admin State
1/0/1	Gigabit - Level	Full	100	Auto	Up
1/0/2	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/3	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/4	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/5	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/6	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/7	Gigabit - Level	N/A	Unknown	Auto	Up
1/0/8	Gigabit - Level	N/A	Unknown	Auto	Up

```

1/0/9   Gigabit - Level           N/A   Unknown  Auto  Up
1/0/10 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/11 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/12 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/13 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/14 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/15 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/16 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/17 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/18 Gigabit - Level           N/A   Unknown  Auto  Up
1/0/19 Gigabit - Level           N/A   Unknown  Auto  Up
--More-- or (q)uit

```

The displayed port configuration information includes the following:

Field	Description
Port	The port number.
Port Type	The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.
Neg	Describes the Auto-negotiation status.
Admin State	Displays whether the port is enabled or disabled.

show interfaces counters

Use the **show interfaces counters** command in either User EXEC mode or Privileged EXEC mode to display Priority Flow Control (PFC) traffic seen by the interface, including Received PFC Frames and Transmitted PFC Frames for a given ethernet or port-channel interface.

Syntax

`show interfaces counters [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, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays traffic seen by the physical interface:

```
console>show interfaces counters
```

Port	InOctets	InUcastPkts
------	----------	-------------

1/0/1	183892	1289
-------	--------	------

3/0/1	123899	1788
-------	--------	------

Port	OutOctets	OutUcastPkts
------	-----------	--------------

1/0/1	9188	9
-------	------	---

2/0/1	0	0
-------	---	---

3/0/1	8789	27
-------	------	----

```

Ch      InOctets      InUcastPkts
-----  -
1       27889            928

```

```

Ch      OutOctets      OutUcastPkts
-----  -
1       23739            882

```

The following example displays counters for Ethernet port 1/0/1.

```
console(config-if-Te1/0/1)#show interfaces counters te1/0/1
```

```

Port      InOctets      InUcastPkts      InMcastPkts      InBcastPkts
-----  -
Te1/0/1   0              0                  0                  0

```

```

Port      OutOctets      OutUcastPkts      OutMcastPkts      OutBcastPkts
-----  -
Te1/0/1   0              0                  0                  0

```

```

FCS Errors: ..... 0
Single Collision Frames: ..... 0
Late Collisions: ..... 0
Excessive Collisions: ..... 0
Multiple Collisions: ..... 0
Oversize Packets: ..... 0
Internal MAC Rx Errors: ..... 0
Received Pause Frames: ..... 0
Transmitted Pause Frames: ..... 0
Received PFC Frames: ..... 0
Transmitted PFC Frames: ..... 0

```

The following table describes the fields shown in the display:

Field	Description
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.
Alignment Errors	A count of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	Counted frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	A count of frames that are involved in a multiple collision, and are subsequently transmitted successfully
Deferred Transmissions	A count of frames for which the first transmission attempt is delayed because the medium is busy
Late Collisions	Counted times that a collision is detected later than one slot time into the transmission of a packet.
Excessive Collisions	Counted frames for which transmission fails due to excessive collisions.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	A count of frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	A count of MAC Control frames received with an opcode indicating the PAUSE operation.

Field	Description
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.
Received PFC Frames	A count of the received Priority Flow Control (PFC) frames.
Transmitted PFC Frames	A count of the transmitted PFC frames.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the description for all interfaces.

```
console>show interfaces description
```

```
Port Description
```

```
-----
```

```
1/0/1 Port that should be used for management only
```

```
2/0/1
```

```
2/0/2
```

```
Ch      Description
```

```
-----
```

```
1      Output
```

show interfaces detail

Use the **show interfaces detail** command in Privileged EXEC mode to display detailed status and configuration of the specified interface.

Syntax

```
show interfaces detail <interface-id>
```

Field	Description
interface-id	A physical interface or port channel identifier.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays detailed status and configuration of the specified interface.

```
console#show interfaces detail gil/0/1
```

```
Port      Type                Duplex  Speed
Neg      Admin  Link
State    State
-----  -----
- - - - -
Gil/0/1Gigabit - Level          N/A     Unknown
Auto  Up      Down

Port      Description
-----  -----
-----
Gil/0/1

Flow Control:Enabled
Port: Gil/0/1
VLAN Membership mode:Access Mode

Operating parameters:
PVID: 1
```

Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
Default Priority: 0
GVRP status:Disabled
Protected:Disabled
Port Gi1/0/1 is member in:

VLAN Type	Name	Egress rule
1 Default	default	Untagged

Static configuration:
PVID: 1
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged

Port Gi1/0/1 is statically configured to:

VLAN	Name	Egress rule
------	------	-------------

Forbidden VLANS:

VLAN	Name
------	------

```

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: 001E.C9AA.AF51
Designated port id: 128.1
Designated path cost: 40000
CST Regional Root: 80:00:00:1E:C9:AA:AF:51  CST
Port Cost: 0
BPDU: sent 121, received 316356

```

show interfaces status

Use the **show interfaces status** command in Privileged EXEC mode to display the status for all configured interfaces.

Syntax

show interfaces status

The displayed port status information includes the following:

Field	Description
Port	The port or port channel number. Oob means Out-of-Band Management Interface.
Name	The port name.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.

Neg	Describes the Auto-negotiation status.
Link State	Displays the Link Aggregation status, either Up or Down .

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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.

Example

The following example displays the status for all configured interfaces.

```
console#show interfaces status
```

Port	Name	Duplex	Speed	Neg	Link State	Flow Control Status
-----	-----	-----	-----	----	-----	-----
Gi1/0/1		N/A	Unknown	Auto	Down	Inactive
Gi1/0/2		N/A	Unknown	Auto	Down	Inactive
Gi1/0/3	ADM-10.0.12.13	N/A	Unknown	Auto	Down	Inactive

show statistics

Use the **show statistics** command in Privileged EXEC mode to display detailed statistics for a specific port or for the entire switch.

Syntax

```
show statistics {gigabitethernet unit/slot/port | switchport | port-channel
port-channel-number | tengigabitethernet unit/slot/port /
fortygigabitethernet unit/slot/port}
```

Parameter Description

Parameter	Description
<i>unit/slot/port</i>	A valid interface. 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following example shows statistics for port I/0/1.

```
console(config-if-Te1/0/1)#show statistics te1/0/1
```

```
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
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0

Total Packets Received Without Errors..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
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..... 0
802.3x Pause Frames Received..... 0
Unacceptable Frame Type..... 0

Total Packets Transmitted (Octets)..... 0
Packets Transmitted 64 Octets..... 0
Packets Transmitted 65-127 Octets..... 0
Packets Transmitted 128-255 Octets..... 0
Packets Transmitted 256-511 Octets..... 0
Packets Transmitted 512-1023 Octets..... 0
Packets Transmitted 1024-1518 Octets..... 0

```



```

Packets Transmitted > 1518 Octets..... 0
Max Frame Size..... 1518

Total Packets Transmitted Successfully..... 0
Unicast Packets Transmitted..... 0
Multicast Packets Transmitted..... 0
Broadcast Packets Transmitted..... 0

Total Transmit Errors..... 0

Total Transmit Packets Discarded..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0

802.3x Pause Frames Transmitted..... 0
GVRP PDUs received..... 0
GVRP PDUs Transmitted..... 0
GVRP Failed Registrations..... 0
BPDU: sent 0, received 0

EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0

Time Since Counters Last Cleared..... 0 day 13 hr
20 min 24 sec

```

show statistics switchport

Use the `show statistics` command in Privileged EXEC mode to display detailed statistics for a specific port or for the entire switch.

Syntax

`show statistics {interface-id | switchport}`

Parameter Description

Parameter	Description
interface-id	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, Config mode and all Config sub-modes

User Guidelines

It is possible to enter interface configuration mode from global configuration mode or from interface configuration mode.

Example

The following example shows statistics for the entire switch.

```
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following example shows storm control configurations for all valid Ethernet ports. The second example shows flow control mode status.

```
console#show storm-control all  
  
          Bcast   Bcast   Mcast   Mcast   Ucast   Ucast  
Intf  Mode   Level  Mode   Level  Mode   Level  
-----  
1/0/1  Disable 5          Disable 5          Disable 5  
1/0/2  Disable 5          Disable 5          Disable 5  
1/0/3  Disable 5          Disable 5          Disable 5  
1/0/4  Disable 5          Disable 5          Disable 5  
console#show storm-control  
802.3x Flow Control Mode..... Disable
```

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-1/0/5)# shutdown
```

The following example re-enables gigabit ethernet port 1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-1/0/5)# 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 | auto [10 | 100 | 1000 | 10000]}
```

```
no speed
```

Parameter Description

Parameter	Description
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 detects the speed it should run based on the port at the other end of the link. If you use the 10, 100, or 1000 keywords with the auto keyword, the port only negotiates at the specified speeds.

Default Configuration

Auto-negotiation is enabled by default on copper ports.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

To disable auto-negotiation on a port, it is necessary to enter both the `speed` and `duplex` commands without using the `auto` parameter. Fiber ports do not support auto-negotiation and therefore require the operator to enter both the `duplex full` command and the `speed` command with the desired operating bandwidth. Disabling auto-negotiation on 1G copper ports may lead to random frame loss as the clock master has not been arbitrated by the auto-negotiation process. Auto-negotiation is required on 10G/40G copper ports, and is always recommended for copper ports. When the `auto` parameter is used 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 do not support auto-negotiation. Both ends of fiber connections must be set to full-duplex and the same speed.

Example

The following example configures the speed operation of Ethernet port 1/0/5 to advertise 100-Mbps operation only.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if)#speed 100
```

storm-control broadcast

Use the **storm-control broadcast** command in Interface Configuration mode to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Syntax

```
storm-control broadcast [level | rate]
```

```
no storm-control broadcast
```

- *level*— The configured rate as a percentage of link-speed.
- *rate*— The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/0/1)#storm-control broadcast
level 5
```

storm-control multicast

Use the **storm-control multicast** command in Interface Configuration mode to enable multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

When you use the **no storm-control multicast** command to "disable" storm-control after having set the level or rate to a non-default value, that value is still set but is not active until you re-enable storm-control.

Syntax

```
storm-control multicast [level | rate]
```

```
no storm-control multicast
```

- *level*— The configured rate as a percentage of link-speed.
- *rate*— The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/0/1)#storm-control multicast
level 5
```


storm-control unicast

Use the **storm-control unicast** command in Interface Configuration mode to enable unknown unicast storm control for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

When you use the **no storm-control multicast** command to "disable" storm-control after having set the level or rate to a non-default value, that value is still set but is not active until you re-enable storm-control.

Syntax

```
storm-control unicast [level | rate]
```

```
no storm-control unicast
```

- *level*— The configured rate as a percentage of link-speed.
- *rate*— The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/0/1)#storm-control unicast level 5
```

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

This command has no user guidelines.

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-1/0/1)#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-if-1/0/1)#switchport protected 1 name
protected
```

show switchport protected

Use the `show switchport protected` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

Ethernet CFM Commands

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 specification deals with the fault diagnosis at service layer across networks comprising multiple LANs, including LANs other than 802.3 media.

PowerConnect 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 Chapter

This chapter explains the following commands:

<code>ethernet cfm domain</code>	<code>ping ethernet cfm</code>
<code>service</code>	<code>traceroute ethernet cfm</code>
<code>ethernet cfm cc level</code>	<code>show ethernet cfm errors</code>
<code>ethernet cfm mep level</code>	<code>show ethernet cfm domain</code>
<code>ethernet cfm mep enable</code>	<code>show ethernet cfm maintenance-points local</code>
<code>ethernet cfm mep active</code>	<code>show ethernet cfm maintenance-points remote</code>

ethernet cfm mep archive-hold-time

show ethernet cfm statistics

ethernet cfm mip level

debug cfm

ethernet cfm domain

Use the **ethernet cfm domain** command in Global Configuration mode to enter into maintenance domain config mode for an existing domain. Use the optional level parameter to create a domain and enter into maintenance domain config mode. In maintenance domain config 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*]

Parameter Description

Parameter	Description	Range	Default	Access
Maintenance domain ID	Unique identifier maintenance domain	0-7 for id	None	Read-write
Maintenance domain name	Name of the maintenance domain	Alphanumeric string of up to 43 characters	None	Read-write

Default Configuration

No CFM domains are pre-configured.

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
console(config-cfm-mdomain)#
```

service

Use the **service** command in maintenance domain config 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 vlanid
```

Parameter Description

Parameter	Description	Range	Default	Access
service	Unique service identifier	alphanumeric string	None	Read-write
Maintenance association VLAN ID	VLAN ID representing a service instance that is monitored by this maintenance association.	1-4093	0	Read-write

Default Configuration

No VLANs are associated with a maintenance domain by default.

Command Mode

Maintenance domain config 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-list* interval *secs*

Parameter Description

Parameter	Description	Range	Default	Access
Maintenance association VLAN ID	VLAN ID representing a service instance that is monitored by this maintenance association.	1-4093	0	Read-write
CCM Interval	Time interval between successive transmissions of CCM.	1, 10, 60, and 600 seconds	1 second	Read-write

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 *1-4093*

Parameter Description

Parameter	Description
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	VLAN on which the MEP operates.

Default Configuration

No MEPs are preconfigured.

Command Mode

Interface Configuration

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 *1-4093* mpid *1-8191*

Parameter Description

Parameter	Description
level	Maintenance association level
mpid	Maintenance entity identifier
vlan	VLAN on which the MEP operates

Default Configuration

No MEPs are preconfigured.

Command Mode

Interface Configuration

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 *1-4093* mpid *1-8191*

Parameter Description

Parameter	Description
level	Maintenance association level
mpid	Maintenance entity identifier
vlan	VLAN on which the MEP operates

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`

Parameter Description

Parameter	Description
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(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*

Parameter Description

Parameter	Description
level	Maintenance association level

Default Configuration

No MIPs are preconfigured.

Command Mode

Interface Configuration

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-gi1/0/1)# ethernet cfm mip level <7>
```

ping ethernet cfm

Use the `ping ethernet cfm` command in Privileged EXEC mode 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]
```

Parameter Description

Parameter	Description
level	Maintenance association level

Parameter	Description
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: 1-4094.
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 in Privileged EXEC mode to generate a link trace message (LTM) from the configured MEP.

Syntax

tracroute ethernet cfm {mac *mac-addr*| remote-mpid *1-8191*} {domain *domain name* | level *0-7*} vlan *vlan-id* mpid *1-8191* [ttl *1-255*]

Parameter Description

Parameter	Description
level	Maintenance association level
mac-addr	The destination MAC address for which the route needs to be traced. Either MEP ID or the MAC address option can be used.
remote-mpid	The MEP ID for which connectivity needs 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: 1-4094.
mpid	The MEP ID from which the link trace message is to be transmitted.
ttl	Number of hops over which the LTM is expected to be transmitted. The default is 64.

Default Configuration

By default, the tracroute 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 # linktrace src-mep 200 target-mep 400 ttl 64
```

show ethernet cfm errors

Use the `show ethernet cfm errors` command in Privileged EXEC mode to display the cfm errors.

Syntax

`show ethernet cfm errors {domain domain-id | level 0-7}`

Parameter Description

Parameter	Description
domain	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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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 in Privileged EXEC mode to display the configured parameters in a maintenance domain.

Syntax

`show ethernet cfm domain {brief | domain-id}`

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display the configured local maintenance points.

Syntax

`show ethernet cfm maintenance-points local {level 0-7 | interface interface-id | domain domain-name}`

Parameter Description

Parameter	Description
domain	Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
level	Maintenance association level
interface-id	Show all MPs associated with the interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
show ethernet cfm maintenance-points local level 1
-----
----
MPID Level Type VLAN Port Direction CC MEP- Operational MAC
              Transmit Active Status
-----
----
1      1      MEP 10   1/0/1  UP    Enabled True
00:02:bc:02:02:02
```

```
-----
Level Type Port MAC
-----
```

show ethernet cfm maintenance-points remote

Use the `show ethernet cfm maintenance-points remote` command in Privileged EXEC mode 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 MEPID] [domain domain-name | level 0-7] [vlan vlan-id] }
```

Parameter Description

Parameter	Description
domain	Name of the maintenance domain (an alphanumeric string of up to 43 characters in length).
level	Maintenance association level
mac-address	The destination MAC address for which the information is desired.
vlan-id	A VLAN associated with the maintenance domain. Range: 1-4094.
mpid	The MEP ID from which the link trace message is to be transmitted.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console# show ethernet cfm maintenance-points remove level 1
```

```
-----  
-----  
MEP Id RMEP Id Level      MAC          VLAN Expiry Timer(sec) Service  
Id  
-----  
-----  
1      2          1      00:11:22:33:44:55 10    25          serv1
```

show ethernet cfm statistics

Use the `show ethernet cfm maintenance-points remote` command in Privileged EXEC mode to display the CFM statistics.

Syntax

```
show ethernet cfm statistics [domain domain-name | level 0-7]
```

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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

```

debug cfm

Use the **debug cfm** command in Privileged EXEC mode to enable CFM debugging. Use the **no** form of the command to disable debugging.

Syntax

```
debug cfm {event | {pdu {all | ccm | ltm | lbm |} {tx | rx}}}
```

Parameter Description

Parameter	Description
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

This command has no user guidelines.

Example

```
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

PowerConnect 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.

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.

Commands in this Chapter

This chapter explains the following commands:

green-mode energy-detect	–
green-mode eee	–

green-mode energy-detect

This command enables a Dell 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 disabled by default on 1G copper interfaces and enabled by default on 10G copper interfaces.

Energy-detect mode is only available on select PowerConnect switches. Refer to your switch data sheet for information about energy-detect mode support.

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). Energy-detect mode cannot be disabled on 10G copper interfaces.

Syntax

```
green-mode energy-detect  
no green-mode energy-detect
```

Parameter Description

This command does not require a parameter description.

Default Configuration

On switches which support energy-detect mode, energy-detect is disabled by default on 1G copper interfaces and enabled by default on 10G copper interfaces.

Command Mode

Interface Configuration mode

User Guidelines

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 and energy-detect modes are only supported on PC81xx 10G ports. Energy-detect mode is always enabled on PC81xx 10G ports and cannot be configured. An error message (`Unable to set energy-detect mode`) will be displayed if the user attempts to configure energy-detect on a 10G port.

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. 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.

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
```

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is **Disabled**.

Command Mode

Interface Configuration

User Guidelines

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 and energy-detect modes are only supported on PC81xx 10G ports.

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}
```

Parameter Description

Parameter	Description
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 PC81xx 10G 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
```


GVRP Commands

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.

Commands in this Chapter

This chapter explains the following commands:

<code>clear gvrp statistics</code>	<code>gvrp vlan-creation-forbid</code>
<code>garp timer</code>	<code>show gvrp configuration</code>
<code>gvrp enable (global)</code>	<code>show gvrp error-statistics</code>
<code>gvrp enable (interface)</code>	<code>show gvrp statistics</code>
<code>gvrp registration-forbid</code>	—

clear gvrp statistics

Use the `clear gvrp statistics` command in Privileged EXEC mode to clear all the GVRP statistics information.

Syntax

```
clear gvrp 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 GVRP statistics information on port 1/0/8.

```
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 centiseconds 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

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-1/0/8)# garp timer leave 90
```

gvrp enable (global)

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)

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

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-1/0/8)#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 has no user guidelines.

Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port 1/0/8.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-1/0/8)#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 has no user guidelines.

Example

The following example disables dynamic VLAN creation on port 1/0/8.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-1/0/8)#gvrp vlan-creation-forbid
```

show gvrp configuration

Use the `show gvrp configuration` command in Privileged EXEC mode 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 [{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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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          Timer          Timer         GVRP Mode    Create Register
              (centiseecs) (centiseecs) (centiseecs) (centiseecs) Forbid Forbid
-----
1/0/1         20             60            1000          Disabled
1/0/2         20             60            1000          Disabled
1/0/3         20             60            1000          Disabled
1/0/4         20             60            1000          Disabled
1/0/5         20             60            1000          Disabled
1/0/6         20             60            1000          Disabled
1/0/7         20             60            1000          Disabled
1/0/8         20             60            1000          Disabled
1/0/9         20             60            1000          Disabled
```

1/0/10	20	60	1000	Disabled
1/0/11	20	60	1000	Disabled
1/0/12	20	60	1000	Disabled
1/0/13	20	60	1000	Disabled
1/0/14	20	60	1000	Disabled

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 [{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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
----	-----	-----	-----	-----	----
1/0/1 0	0	0	0	0	
1/0/2 0	0	0	0	0	
1/0/3 0	0	0	0	0	
1/0/4 0	0	0	0	0	

show gvrp statistics

Use the `show gvrp statistics` command in User EXEC mode to display GVRP statistics.

Syntax

```
show gvrp 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

This example shows output of the **show gvrp statistics** command.

```
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
```

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
----	---	----	----	----	---	---	---	---	---	----	----	---
1/0/1	0	0	0	0	0	0	0	0	0	0	0	0
1/0/2	0	0	0	0	0	0	0	0	0	0	0	0
1/0/3	0	0	0	0	0	0	0	0	0	0	0	0
1/0/4	0	0	0	0	0	0	0	0	0	0	0	0
1/0/5	0	0	0	0	0	0	0	0	0	0	0	0
1/0/6	0	0	0	0	0	0	0	0	0	0	0	0
1/0/7	0	0	0	0	0	0	0	0	0	0	0	0
1/0/8	0	0	0	0	0	0	0	0	0	0	0	0

IGMP Snooping Commands

Snooping of Internet Group Management Protocol (IGMP) messages is a feature that allows PowerConnect switches to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. 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 PowerConnect 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 Chapter

This chapter explains the following commands:

<code>ip igmp snooping (global)</code>	<code>show ip igmp snooping interface</code>
<code>ip igmp snooping (interface)</code>	<code>show ip igmp snooping mrouter</code>
<code>ip igmp snooping host-time-out</code>	<code>ip igmp snooping (VLAN)</code>
<code>ip igmp snooping leave-time-out</code>	<code>ip igmp snooping fast-leave</code>
<code>ip igmp snooping mrouter-time-out</code>	<code>ip igmp snooping groupmembership-interval</code>
<code>show ip igmp snooping</code>	<code>ip igmp snooping maxresponse</code>
<code>show ip igmp snooping groups</code>	<code>ip igmp snooping mcrtexpiretime</code>

ip igmp snooping (global)

Use the `ip igmp snooping` command in Global Configuration mode to globally enable Internet Group Management Protocol (IGMP) snooping. Use the `no` form of this command to disable IGMP snooping globally.

Syntax

`ip igmp snooping`

`no ip igmp snooping`

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping is enabled on static VLANs only and is not enabled on Private VLANs or their community VLANs.

Example

The following example globally enables IGMP snooping.

```
console(config)# ip igmp snooping
```

ip igmp snooping (interface)

Use the **ip igmp snooping** command in Interface Configuration mode to enable Internet Group Management Protocol (IGMP) snooping on a specific interface. To disable IGMP snooping on an Ethernet interface, use the **no** form of this command.

Syntax

```
ip igmp snooping
```

```
no ip igmp snooping
```

Default Configuration

IGMP snooping is disabled.

Command Mode

Interface Configuration (*gigabitethernet*, *port-channel*, *tengigabitethernet*, *fortygigabitethernet*) mode

User Guidelines

IGMP snooping can be enabled on Ethernet interfaces.

Example

The following example enables IGMP snooping.

```
console(config-if-1/0/1)#ip igmp snooping
```

ip igmp snooping host-time-out

Use the `ip igmp snooping host-time-out` command in Interface Configuration mode to configure the host-time-out. If an IGMP report for a Multicast group is not received for a host time-out period from a specific port, this port is deleted from the member list of that Multicast group. To reset to the default host time-out, use the `no` form of this command.

Syntax

`ip igmp snooping host-time-out time-out`

`no ip igmp snooping host-time-out`

- *time-out* — Host time-out in seconds. (Range: 2- 3600)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (`gigabitethernet`, `port-channel`, `tengigabitethernet`, `fortygigabitethernet`) mode

User Guidelines

The time-out should be more than sum of response time and twice the query interval.

Example

The following example configures the host time-out to 300 seconds.

```
console(config-if-1/0/1)#ip igmp snooping host-time-out 300
```

ip igmp snooping leave-time-out

Use the `ip igmp snooping leave-time-out` command in Interface Configuration mode to configure the leave-time-out. If an IGMP report for a Multicast group is not received within the leave-time-out period after an

IGMP leave was received from a specific port, the current port is deleted from the member list of that Multicast group. To configure the default leave-time-out, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out [*time-out* | **immediate-leave**]

no ip igmp snooping leave-time-out

- *time-out* — Specifies the leave-time-out in seconds. (Range: 1-25)
- **immediate-leave** — Specifies that the port should be removed immediately from the members list after receiving IGMP Leave.

Default Configuration

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

The leave time-out should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.

Use **immediate leave** only where there is only one host connected to a port.

Example

The following example configures the host leave-time-out to 15 seconds.

```
console(config-if-1/0/1)#ip igmp snooping leave-time-out 15
```

ip igmp snooping mrouter-time-out

Use the **ip igmp snooping mrouter-time-out** command in Interface Configuration mode to configure the mrouter-time-out. This command is used for setting the aging-out time after Multicast router ports are automatically learned. To reset to the default mrouter-time-out, use the **no** form of this command.

Syntax

`ip igmp snooping mrouter-time-out time-out`

`no ip igmp snooping mrouter-time-out`

- *time-out* — mrouter time-out in seconds for IGMP. (Range: 1–3600)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (`gigabitethernet`, `port-channel`, `tengigabitethernet`, `fortygigabitethernet`) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the mrouter time-out to 200 seconds.

```
console(config-if-1/0/1)#ip igmp snooping mrouter-  
time-out 200
```

show ip igmp snooping

Use the `show ip igmp snooping` command in Privileged EXEC mode to display the IGMP snooping configuration.

Syntax

`show ip igmp snooping [vlan vlan-id]`

Parameter Description

Parameter	Description
vlan-id	Specifies a VLAN ID value (available only in Privileged EXEC mode).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The example shows Multicast groups learned by IGMP snooping for all VLANs.

```
console>show ip igmp snooping groups
Vlan      IP Address                Ports
```

1	224-239.130 2.2.3	1/0/1, 2/0/2
19	224-239.130 2.2.8	1/0/9-1/0/11

IGMP Reporters that are forbidden statically:

Vlan	IP Address	Ports
1	224-239.130 2.2.3	1/0/19

show ip igmp snooping interface

Use the `show ip igmp snooping interface` command in Privileged EXEC mode to display the IGMP snooping configuration.

Syntax

```
show ip igmp snooping interface 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

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The example displays IGMP snooping information.

```
console#show ip igmp snooping interface 1/0/1
```



```

Slot/Port..... 1/0/1
IGMP Snooping Admin Mode..... Disabled
Fast Leave Mode..... Disabled
Group Membership Interval..... 260
Max Response Time..... 10
Multicast Router Present Expiration Time.... 300

```

show ip igmp snooping mrouter

Use the `show ip igmp snooping mrouter` command in Privileged EXEC mode 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 modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows IGMP snooping mrouter information.

```

console#show ip igmp snooping mrouter
Port.....1/0/1

```

ip igmp snooping (VLAN)

Use the `ip igmp snooping` command in VLAN Configuration mode to enable IGMP snooping on a particular interface or on all interfaces participating in a VLAN. To disable IGMP snooping use the `no` form of this command.

Syntax

```
ip igmp snooping vlan-id  
no ip igmp snooping
```

Default Configuration

IGMP snooping is disabled on VLAN interfaces by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping on VLAN 2.

```
console#vlan database  
console(config-vlan)#ip igmp snooping 2
```

ip igmp snooping fast-leave

This command enables or disables IGMP Snooping fast-leave mode on a selected VLAN. Enabling fast-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 fast-leave mode on a VLAN.

You should enable fast-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, fast-leave processing is supported only with IGMP version 2 hosts.

Syntax

```
ip igmp snooping fast-leave vlan-id
```

```
no ip igmp snooping fast-leave
```

- *vlan id*— Number assigned to the VLAN.

Default Configuration

IGMP snooping fast-leave mode is disabled on VLANs by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping fast-leave mode on VLAN 2.

```
console(config-vlan)#ip igmp snooping fast-leave 2
```

ip igmp snooping groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN. 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.

Syntax

`ip igmp snooping groupmembership-interval vlan-id seconds`

`no ip igmp snooping groupmembership-interval`

- *vlan-id* — Number assigned to the VLAN
- *seconds* — IGMP group membership interval time in seconds. (Range: 2–3600)

Default Configuration

The default group membership interval time is 260 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an IGMP snooping group membership interval of 520 seconds.

```
console(config-vlan)#ip igmp snooping
groupmembership-interval 2 520
```

ip igmp snooping maxresponse

This command sets the IGMP Maximum Response time on a particular VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. 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 maximum response time on the VLAN to the default value.

Syntax

`ip igmp snooping maxresponse vlan-id seconds`

`no ip igmp snooping maxresponse vlan-id`

- *vlan-id*— Number assigned to the VLAN.
- *seconds*— IGMP Maximum response time in seconds. (Range: 1-25)

Default Configuration

The default maximum response time is 10 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

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 25 seconds on VLAN 2.

```
console(config-vlan)#ip igmp snooping maxresponse 25
```

ip igmp snooping mcruntime

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. The time is set for a particular VLAN.

Syntax

`ip igmp snooping mcruntime vlan-id seconds`

`no ip igmp mcruntime vlan-id`

- *vlan id*— Number assigned to the VLAN
- *seconds*— Multicast router present expiration time. (Range: 1–3600)

Default Configuration

The default multicast router present expiration time is 300 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

The mcrexpiretime 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-vlan)#ip igmp mcrtexpiretime 2 60
```

IGMP Snooping Querier Commands

The IGMP/MLD Snooping Querier is an extension to the IGMP/MLD Snooping feature. IGMP/MLD Snooping Querier allows the switch to simulate an IGMP/MLD router in a Layer 2-only network, thus removing the need to have an IGMP/MLD Router to collect and refresh the multicast group membership information. The querier function simulates a small subset of the IGMP/MLD router functionality.

In a network with IP multicast routing, an IP multicast router acts as the IGMP/MLD querier. However, if it is required that the IP-multicast traffic in a VLAN be switched, the PowerConnect can be configured as an IGMP/MLD querier. When IGMP/MLD Snooping Querier is enabled, the Querier sends out periodic IGMP/MLD General Queries that trigger the Multicast listeners/member to send their joins so as to receive the Multicast data traffic. IGMP/MLD Snooping listens to these reports to establish the appropriate L2 forwarding table entries.

The PowerConnect supports version IGMP V1 and 2 for snooping IGMP queries.

Commands in this Chapter

This chapter explains the following commands:

<code>ip igmp snooping querier</code>	<code>ip igmp snooping querier timer expiry</code>
<code>ip igmp snooping querier election participate</code>	<code>ip igmp snooping querier version</code>
<code>ip igmp snooping querier query-interval</code>	<code>show ip igmp snooping querier</code>

ip igmp snooping querier

This command enables or disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN. 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 it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping Querier functionality is re-enabled if IGMP Snooping is operational on the VLAN.

The IGMP Snooping Querier application sends periodic general queries on the VLAN to solicit membership reports.

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 disables itself if it detects IGMP traffic from a multicast-enabled router.

Command Mode

Global Configuration mode

User Guidelines

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 use the management IP address as the IGMP snooping querier source address. Using all zeros for the querier IP address removes it. The VLAN IP address takes precedence over the global IP address.

Example

The following example enables IGMP snooping querier in VLAN Configuration mode.

```
console(config-vlan)#ip igmp snooping querier 1  
address 10.19.67.1
```

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 Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier source address is more than the Snooping Querier address, it stops sending periodic queries. If the Snooping Querier wins the election, then it continues sending periodic queries. The **no** form of this command sets the snooping querier not to participate in the querier election but to go into a non-querier mode as soon in as it discovers the presence of another querier in the same VLAN.

Syntax

ip igmp snooping querier election participate *vlan-id*

no ip igmp snooping querier election participate *vlan-id*

Default Configuration

The snooping querier is configured to not participate in the querier election by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the snooping querier to participate in the querier election.

```
console#vlan database
```

```
console(config-vlan)#ip igmp snooping querier  
election participate
```

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 Snooping Max Response Time.

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]`

Syntax Description

Parameter	Description
<code>vlan_id</code>	Specifies a VLAN ID value.

When the optional argument *vlan_id* is not used, the command shows the following information.

Parameter	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	Indicates the version of IGMP that will be used while sending out the queries.
Source IP Address	Shows the IP address that is used in the IPv4 header when sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlan_id*, the following information appears.

Parameter	Description
VLAN Admin Mode	Indicates whether IGMP Snooping Querier is active on the VLAN.
VLAN Operational State	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.
VLAN Operational Max Response Time	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.
Querier Election Participate	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

Parameter	Description
Elected Querier	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.

When the optional argument detail is used, the command shows the global information and the information for all Querier enabled VLANs.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged Exec modes

User Guidelines

This command has no user guidelines.

Example

The following example shows querier information for VLAN 2.

```
console#show ip igmp snooping querier vlan 2
```

```
Vlan 2 :    IGMP Snooping querier status
```

```
-----
IGMP Snooping Querier Vlan Mode..... Enable
Querier Election Participate Mode..... Disable
Querier Vlan Address..... 0.0.0.0
Operational State..... Non-Querier
Last Querier Address..... 2.2.2.2
Operational version..... 3
Operational Max Resp Time..... 11
```

IP Addressing Commands

Interfaces on the PowerConnect switches support a variety of capabilities to support management of the switch. In addition to performing switching and routing of network traffic, PowerConnect 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 PowerConnect 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 Chapter

This chapter explains the following commands:

<code>clear host</code>	<code>ip host</code>
<code>clear ip address-conflict-detect</code>	<code>ip name-server</code>
<code>-</code>	<code>ipv6 address (Interface Config)</code>
<code>ip address (Out-of-Band)</code>	<code>ipv6 address dhcp</code>
<code>ip address-conflict-detect run</code>	<code>ipv6 enable (Interface Config)</code>
<code>ip address dhcp (Interface Config)</code>	<code>show hosts</code>
<code>ip default-gateway</code>	<code>show ip address-conflict</code>
<code>ip domain-lookup</code>	<code>show ip helper-address</code>
<code>ip domain-name</code>	<code>-</code>

clear host

Use the **clear host** command in Privileged EXEC mode 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 in Privileged EXEC mode to clear the address conflict detection status in the switch.

Syntax

```
clear ip address-conflict-detect
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#  
console#configure  
console(config)#clear ip address-conflict-detect
```

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}  
no ip address
```

Parameter Description

Parameter	Description
<i>ip-address</i>	Specifies a valid IP address.
<i>mask</i>	Specifies a valid subnet (network) mask IP address.
<i>prefix-length</i>	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 service port.

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.

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
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

Example

```
console#  
console#configure  
console(config)#ip address-conflict-detect run
```

ip address dhcp (Interface Config)

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
```

Parameter Description

This command does not require a parameter description.

Default Configuration

DHCPv4 is disabled by default on routing interfaces.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

This command only applies to 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 dhcp** 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** 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.

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 in Global Configuration mode to configure a default gateway (router).

Syntax

`ip default-gateway ip-address`

`no ip default-gateway ip-address`

Parameter Description

Parameter	Description
<i>ip-address</i>	Valid IPv4 address of an attached router.

Default Configuration

No default gateway is defined.

Command Mode

Global 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.

Example

The following example sets the default-gateway to 10.1.1.1.

```
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.

```
console(config)#ip host accounting.dell.com
176.10.23.1
```

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 on page 523 to display the configured name servers.

Example

The following example sets the available name server.

```
console (config) #ip name-server 176.16.1.18
```

ipv6 address (Interface Config)

Use the **ipv6 address** command to set the IPv6 address of the management interface. Use the **no** form of this command to reset the IPv6 address to the default.

Syntax

```
ipv6 address {prefix/prefix-length [eui64] | autoconfig | dhcp}
```

```
no ipv6 address
```

- *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.
- **autoconfig**—Use this keyword to set the 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, loopback, port-channel)

User Guidelines

When setting the prefix length on an IPv6 address, no space can be present between the address and the mask.

Example

Configure ipv6 routing on vlan 10 and obtain an address via DHCP. Assumes vlan 10 already exists.

```
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) Config 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}`

Parameter Description

Parameter	Description
<code>prefix/prefix-length</code>	An IPv6 prefix in global format address format.
<code>eui64</code>	Formulate the prefix in EUI-64 format.
<code>autoconfig</code>	Perform IPv6 auto-configuration.
<code>dhcp</code>	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.

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
```

Parameter Description

This command does not require a parameter description.

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.

```
console#config
```

```
console(config)#interface vlan2
```

```
console(config-if-vlan2)#ipv6 address dhcp
```

ipv6 enable (Interface Config)

Use the `ipv6 enable` command in Interface Config 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, loopback)

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#no ipv6 enable
```

ipv6 enable (OOB Config)

Use the `ipv6 enable` command in Interface (out-of-band) Config 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

There are no user guidelines for this command.

ipv6 gateway (OOB Config)

Use the `ipv6 gateway` command in Interface (out-of-band) Config 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
```

Parameter Description

Parameter	Description
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

There are no user guidelines for this command.

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. The command itself shows hosts [hostname].

- Host name. (Range: 1–255 characters). The command allows spaces in the host name when specified in double quotes. For example, console(config)#snmp-server host "host name"

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays information about IP hosts.

```
console>show hosts
Host name:
Default domain: gm.com, sales.gm.com, usa.sales.gm.com
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:
Host                               Addresses
-----
accounting.gm.com                  176.16.8.8
Cache:                               TTL (Hours)
Host                               Total    Elapsed    Type    Addresses
-----
www.stanford.edu                   72      3          IP      171.64.14.203
```

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`

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

The command provides the following information.

Term	Description
Address Conflict Detection Status	Whether the switch has detected an address conflict on any IP address. Set to Conflict Detected if detected, No Conflict Detected otherwise.
Last Conflicting IP Address	The IP address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes, and seconds since the last address conflict was detected.

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 in Privileged EXEC mode to display IP helper addresses configuration.

Syntax

```
show ip helper-address [intf-address]
```

- *intf-address* — IP address of a routing interface. (Range: Any valid IP address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip helper-address
```

IP helper is enabled

Interface Server Address	UDP Port	Discard	Hit Count
----- -----			
vlan 25 192.168.40.2	domain	No	0
vlan 25 192.168.40.2	dhcp	No	0
vlan 30	dhcp	Yes	0
vlan 30 192.168.23.1	162	No	0
Any 192.168.40.1	dhcp	No	0

show ipv6 dhcp interface out-of-band statistics

Use the `show ipv6 dhcp interface out-of-band statistics` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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 in Privileged EXEC mode to show the IPv6 out-of-band port configuration.

Syntax

`show ipv6 interface out-of-band`

Parameter Description

Parameter	Description
ipv6-address	An IPv6 address (not a prefix).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console(config-if)#do 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 AutoConfig Mode.....Enabled
Burned In MAC Address.....001E.C9AA.AD79
```

IPv6 Access List Commands

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 PowerConnect 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 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 physical ports and LAGs. ACLs can also be time based.

Commands in this Chapter

This chapter explains the following commands:

deny permit (IPv6 ACL)	ipv6 traffic-filter
ipv6 access-list	show ipv6 access-lists
ipv6 access-list rename	–

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.

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.

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.

Syntax

```
{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | protocolnumber}
{any | sourceipv6prefix/prefixlength} [eq {portnumber | portkey}] {any |
destinationipv6prefix/prefixlength}] [eq {portnumber | portkey}] [flow-
label flow-label-value] [dscp dscp-value]} [assign-queue queue-id] [log]
[{mirror | redirect} interface-id] [time-range time-range-name]
```

Parameter Description

Parameter	Description
deny permit	Specifies whether the IP ACL rule permits or denies an action.

Parameter	Description
every	Allows all protocols.
icmpv6 ipv6 tcp udp <i>protocolnumber</i>	Protocol to match, specified as keywords icmp, igmp, ipv6, tcp, udp or as a standard protocol number from 1–255.
any <i>sourceipv6</i> <i>prefix/</i> <i>prefixlength</i>	any matches any source IP address. Or, you can specify a source IPv6 address expressed as a prefix/prefixlength.
eq { <i>portnumber</i> <i>portkey</i> }	eq matches a port number being used as a match criteria. The first reference provides the source match criteria and the second provides destination match criteria. The <i>portnumber</i> variable must be in the range 0–65535. Or you can specify one of the values as the <i>portkey</i> : domain, echo, efts, ftpdata, http, smtp, snmp, telnet, tftp, and www.
any <i>destinationipv6</i> <i>prefix/</i> <i>prefixlength</i>	any matches any source IP address. Or, you can specify a source IPv6 address expressed as a prefix/prefixlength.
flow label <i>flow-label-</i> <i>value</i>	The value to match in the Flow Label field of the IPv6 header (Range 0–1048575).
dscp <i>dscp-value</i>	Specifies the TOS for an IPv6 ACL rule depending on a match of DSCP values using the parameter <i>dscp</i> .
assign-queue <i>queue-</i> <i>id</i>	Specifies particular hardware queue for handling traffic that matches the rule. (Range: 0-6)
log	Specifies that this rule is to be logged.
mirror <i>interface</i>	Allows the traffic matching this rule to be copied to the specified interface.
redirect <i>interface</i>	This parameter allows the traffic matching this rule to be forwarded to the specified interface.
time-range-name	Use the time-range parameter to impose a time limitation on the IPv6 ACL rule as defined by the parameter <i>time-range-name</i> .

Default Configuration

This command has no default configuration.

Command Mode

IPv6-Access-List Configuration mode

User Guidelines

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.

The 'no' form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and re specified.

Example

The following example creates rules in an IPv6 ACL named "STOP_HTTP" to discard any HTTP traffic from the 2001:DB8::/32 network, but allow all other traffic from that network:

```
console(config)#ipv6 access-list STOP_HTTP
console(Config-ipv6-acl)#deny ipv6 2001:DB8::/32 any
eq http
console(Config-ipv6-acl)#permit ipv6 2001:DB8::/32
any
console(Config-ipv6-acl)#
```

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. 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 config mode to update the existing IPv6 ACL.

Use the **no** form of the command to delete an IPv6 ACL from the system.

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

There are no user guidelines for this command

Example

The following example creates an IPv6 ACL named "DELL_IP6" and enters the IPv6-Access-List Config 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.

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.

Use the “no” form of the command to remove an IPv6 ACL from the interface(s) in a given direction.

Syntax

```
ipv6 traffic-filter name direction [sequence seq-num]
```

```
no ipv6 traffic-filter name direction
```

- **name** — Alphanumeric string of 1 to 31 characters uniquely identifying the IPv6 access list.
- **direction** — Direction of the ACL. (Range: in or out)

- **sequence *seq-num*** — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1–4294967295)

Default Configuration

This command has no default configuration.

Command Modes

Global Configuration mode

Interface Configuration (Ethernet, Port-channel, VLAN) mode

User Guidelines

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces.

Example

The following example attaches an IPv6 access control list to an interface.

```
console(config-if-1/0/1)#ipv6 traffic-filter DELL_IP6
in
```

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]
```

Parameter Description

Parameter	Description
<i>name</i>	The name used to identify the IPv6 ACL.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.

Parameter	Description
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

The following example displays configuration information for the IPv6 ACLs.

```
console#show ipv6 access-lists
```

```
Current number of all ACLs: 1 Maximum number of all
ACLs: 100
```

```

      IPv6 ACL Name          Rules Direction
Interface(s)              VLAN(s)
-----
STOP_HTTP                2      inbound  1/0/1
```

```
console#show ipv6 access-lists STOP_HTTP
```

```
ACL Name: STOP_HTTP
```

Inbound Interface(s) : 1/0/1

Rule Number: 1

Action..... deny

Protocol.....
255 (ipv6)

Source IP Address.....
2001:DB8::/32

Destination L4 Port Keyword.....
80 (www/http)

Rule Number: 2

Action.....
permit

Protocol.....
255 (ipv6)

Source IP Address..... 2001:DB8::/32

The command output provides the following information:

Field	Description
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	This displays the protocol to filter for this rule.
Source IP Address	This displays the source IP address for this rule.

Source L4 Port Keyword	This field displays the source port for this rule.
Destination IP Address	This displays the destination IP address for this rule.
Destination L4 Port Keyword	This field displays the destination port for this rule.
IP DSCP	This field indicates the value specified for IP DSCP.
Flow Label	This field indicates the value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Mirror Interface	Displays the interface to which packets matching this rule are copied.
Redirect Interface	Displays the interface to which packets matching this rule are forwarded.

IPv6 MLD Snooping Commands

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.

PowerConnect 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 PowerConnect implementation is compliant to RFC 4541.

Commands in this Chapter

This chapter explains the following commands:

<code>ipv6 mld snooping immediate-leave</code>	<code>ipv6 mld snooping (Interface)</code>
<code>ipv6 mld snooping groupmembership-interval</code>	<code>ipv6 mld snooping (VLAN)</code>
<code>ipv6 mld snooping maxresponse</code>	<code>show ipv6 mld snooping</code>
<code>ipv6 mld snooping mrcexpiretime</code>	<code>show ipv6 mld snooping groups</code>
<code>ipv6 mld snooping (Global)</code>	—

ipv6 mld snooping immediate-leave

The `ipv6 mld snooping immediate-leave` command enables or disables MLD Snooping `snooping immediate-leave admin` mode on a selected interface or VLAN. Enabling `fast-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. You should enable `fast-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, `fast-leave` processing is supported only with MLD version 1 hosts.

Syntax

```
ipv6 mld snooping immediate-leave [vlan-id]
```

```
no ipv6 mld snooping immediate-leave [vlan-id]
```

- `vlan_id` — Specifies a VLAN ID value in VLAN Database mode.

Default Configuration

MLD Snooping `fast-leave` mode is disabled.

Command Mode

Interface Configuration (`gigabitethernet`, `port-channel`, `tengigabitethernet`, `fortygigabitethernet`) mode.

VLAN Database Mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-vlan)#ipv6 mld snooping immediate-leave 4
```


ipv6 mld snooping groupmembership-interval

The `ipv6 mld snooping 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 groupmembership-interval [vlan-id] [seconds]`

`no ipv6 mld snooping groupmembership-interval [vlan-id]`

- `vlan_id` — Specifies a VLAN ID value in VLAN Database mode.
- `seconds` — MLD group membership interval time in seconds. (Range: 2-3600)

Default Configuration

The default group membership interval time is 260 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-4/0/1)#ipv6 mld snooping
groupmembership-interval 300
```

ipv6 mld snooping maxresponse

The `ipv6 mld snooping maxresponse` command sets the MLD Maximum Response time for an interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an

interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 3599 seconds.

Syntax

```
ipv6 mld snooping maxresponse [vlan-id] [seconds]
```

```
no ipv6 mld snooping maxresponse [vlan-id]
```

- `vlan_id` — Specifies a VLAN ID value in VLAN Database mode.
- `seconds` — MLD maximum response time in seconds. (Range: 1–3599)

Default Configuration

The default maximum response time is 10 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-4/0/1)#ipv6 mld snooping  
maxresponse 33
```

ipv6 mld snooping mcrtexpiretime

The `ipv6 mld snooping mcrtexpiretime` command sets the Multicast Router Present Expiration time. 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.

Syntax

```
ipv6 mld snooping mcrtexpiretime [vlan-id] [seconds]
```

`no ipv6 mld snooping mrcexpiretime [vlan-id]`

- *vlan_id*— Specifies a VLAN ID value in VLAN Database mode.
- *seconds*— multicast router present expiration time in seconds. (Range: 1–3600)

Default Configuration

The default multicast router present expiration time is 300 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines

Example

```
console(config-if-4/0/1)#ipv6 mld snooping  
mrcexpiretime 60
```

ipv6 mld snooping (Global)

The `ipv6 mld snooping (Global)` command enables MLD Snooping on the system (Global Config Mode).

Syntax

`ipv6 mld snooping`

`no ipv6 mld snooping`

Default Configuration

MLD Snooping is disabled.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 mld snooping
```

ipv6 mld snooping (Interface)

The `ipv6 mld snooping (Interface)` command enables MLD Snooping on an interface. If an interface has MLD Snooping enabled and it becomes a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if the interface is removed from a port-channel (LAG).

Syntax

```
ipv6 mld snooping
```

```
no ipv6 mld snooping
```

Default Configuration

MLD Snooping is disabled.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, *fortygigabitethernet*) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-4/0/1)#ipv6 mld snooping
```

ipv6 mld snooping (VLAN)

The `ipv6 mld snooping (VLAN)` command enables MLD Snooping on a particular VLAN and enables MLD snooping on all interfaces participating in a VLAN.

Syntax

```
ipv6 mld snooping vlan-id
```

```
no ipv6 mld snooping vlan-id
```

- *vlan-id*— Specifies a VLAN ID value.

Default Configuration

MLD Snooping is disabled.

Command Mode

VLAN Database mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-vlan)#ipv6 mld snooping 1
```

show ipv6 mld snooping

The `show ipv6 mld snooping` command displays MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Syntax

```
show ipv6 mld snooping [interface {{gigabitethernet unit/slot/port | port-channel port-channel-number | tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port}} | vlan vlan-id]
```

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

With no optional arguments, the command displays the following information:

- Admin Mode — Indicates whether or not MLD Snooping is active on the switch.
- Interfaces Enabled for MLD Snooping — Interfaces on which MLD Snooping is enabled.
- MLD Control Frame Count — This displays the number of MLD control frames that are processed by the CPU.
- VLANs Enabled for MLD Snooping — VLANs on which MLD Snooping is enabled.

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.
- Max Response Time — 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.

show ipv6 mld snooping groups

The `show ipv6 mld snooping groups` command displays the MLD Snooping entries in the MFDB table.

Syntax

`show ipv6 mld snooping groups` [`{vlan vlan-id | address ipv6-multicast-address}`]

- *vlan_id* — Specifies a VLAN ID value.
- *ipv6-multicast-address* — Specifies an IPv6 Multicast address.

Default configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 mld snooping groups
```

Vlan	Ipv6 Address	Type	Ports
1	3333.0000.0003	Dynamic	1/0/1,1/0/3
2	3333.0000.0004	Dynamic	1/0/1,1/0/3
2	3333.0000.0005	Dynamic	1/0/1,1/0/3

MLD Reporters that are forbidden statically:

```
-----
```

Vlan	Ipv6 Address	Ports
------	--------------	-------

```
-----
```

```
console#show ipv6 mld snooping groups vlan 2
```

Vlan	Ipv6 Address	Type	Ports
2	3333.0000.0004	Dynamic	1/0/1,1/0/3
2	3333.0000.0005	Dynamic	1/0/1,1/0/3

```
MLD Reporters that are forbidden statically:
```

```
-----
```

Vlan	Ipv6 Address	Ports
------	--------------	-------

```
-----
```


IPv6 MLD Snooping Querier Commands

IGMP/MLD Snooping Querier is an extension of the IGMP/MLD Snooping feature. IGMP/MLD Snooping Querier allows the switch to simulate an IGMP/MLD router in a Layer 2-only network, thus removing the need to have an IGMP/MLD Router to collect the multicast group membership information. The querier function simulates a small subset of the IGMP/MLD router functionality.

In a network with IP multicast routing, the IP multicast router acts as the IGMP/MLD querier. However, if it is required that the IP-multicast traffic in a VLAN be switched, the switch can be configured as an IGMP/MLD querier. When IGMP/MLD Snooping Querier is enabled, the Querier sends out periodic IGMP/MLD General Queries that trigger the Multicast listeners/member to send their joins so as to receive the Multicast data traffic. IGMP/MLD Snooping listens to these reports to establish the appropriate forwarding table entries.

PowerConnect switches support IGMP V1 and 2 for snooping IGMP queries.

Commands in this Chapter

This chapter explains the following commands:

<code>ipv6 mld snooping querier</code>	<code>ipv6 mld snooping querier query-interval</code>
<code>ipv6 mld snooping querier (VLAN mode)</code>	<code>ipv6 mld snooping querier timer expiry</code>
<code>ipv6 mld snooping querier address</code>	<code>show ipv6 mld snooping querier</code>
<code>ipv6 mld snooping querier election participate</code>	–

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

There are no user guidelines for this command.

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-id
no ipv6 mld snooping querier vlan-id
```

- *vlan-id*— A valid VLAN ID. (Range: 1–4093)

Default Configuration

MLD Snooping Querier is disabled by default on all VLANs.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-vlan)#ipv6 mld snooping querier 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* — 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.

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. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is higher than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election then it will continue sending periodic queries. 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 valid VLAN ID. (Range: 1 - 4093)

Default Configuration

Election participation is disabled by default.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

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. It is the amount of time in seconds that the switch waits before sending another general query. 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

There are no user guidelines for this command

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. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network. 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

There are no user guidelines for this command.

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 valid VLAN ID. (Range: 1 - 4093)

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

When the optional argument `vlan vlan-id` is not used, the command shows the following information:

Parameter	Description
-----------	-------------

MLD Snooping Querier Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Querier Address	Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.
MLD Version	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.
Querier Query Interval	Shows the amount of time that a Snooping Querier waits before sending out a periodic general query.
Querier Expiry Interval	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When the optional argument `vlan vlan-id` is used, the following additional information appears:

Parameter	Description
MLD Snooping Querier VLAN Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
Querier Election Participate Mode	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.
Operational State	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.
Operational Version	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.

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

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 physical and LAG 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 Chapter

This chapter explains the following commands:

[ip verify source](#)

[show ip verify interface](#)

[ip verify source port-security](#)

[show ip verify source interface](#)

[ip verify binding](#)

[show ip source binding](#)

ip verify source

Use the **ip verify source** command in Interface Configuration mode to enable filtering of IP packets matching the source IP address.

Syntax

`ip verify source`

Default Configuration

By default, IPSG is disabled on all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-Gi1/0/1)#ip verify source
```

ip verify source port-security

Use the `ip verify source port-security` command in Interface Configuration mode to enable filtering of IP packets matching the source IP address and the source MAC address.

Syntax

`ip verify source port-security`

Default Configuration

By default, IPSG is disabled on all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/0/1)#ip verify source port-  
security
```

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 will not be any static bindings configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

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 interface

Use the **show ip verify interface** command in Privileged EXEC mode to display the IPSG interface configuration.

Syntax

```
show ip verify interface
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip verify interface gigabitethernet  
1/0/1
```

show ip verify source interface

Use the `show ip verify source interface` command in Privileged EXEC mode to display the bindings configured on a particular interface.

Syntax

```
show ip verify source interface
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip verify source interface  
gigabitethernet 1/0/1
```

show ip source binding

Use the `show ip source binding` command in Privileged EXEC mode to display all bindings (static and dynamic).

Syntax

`show ip source binding`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip source binding
```


iSCSI Optimization Commands

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 homogenous 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. Each monitored iSCSI session utilizes two rules from additional ACL lists up to a maximum of two ACL lists. This means that the maximum number of ACL lists allocated by iSCSI is three.

Commands in this Chapter

This chapter explains the following commands:

iscsi aging time	iscsi target port
iscsi cos	show iscsi
iscsi enable	show iscsi sessions

iscsi aging time

The `iscsi aging time` command sets the time out value for iSCSI sessions. To reset the aging time to the default value, use the `no` form of this command.

Syntax

`iscsi aging time time`

`no iscsi aging time`

- *time* — The number of minutes a session must not be active prior to it's removal. (Range: 1 43,200)

Default Configuration

The default aging time is 10 minutes.

Command Mode

Global Configuration mode.

User Guidelines

Changing the aging time has the following behavior:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Example

The following example sets the aging time for iSCSI sessions to 100 minutes.

```
console(config)#iscsi aging time 100
```

iscsi cos

The `iscsi cos vpt` command is supported on the PowerConnect PC8024/PC8164/PC8164F/.

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
```

Parameter Description

Parameter	Description
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.

Parameter	Description
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 dot1p mapping assigns to queue 2.

Command Mode

Global Configuration mode.

User Guidelines

The remark option only applies to DSCP values. Remarking is not available for vpt values.

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.

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.

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 10 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 also 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.

Enabling iSCSI will force the sending of the DCBX Application Priority TLV to a port with the following parameters when the following conditions are met:

- DCBX is enabled
- CoS Queuing is enabled on the port using VPT

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 or FCoE application priority information, it is not necessary to enable `iscsi cos` to send the iSCSI Application Priority TLV.

Example

In the following example, iSCSI is globally enabled.

```
console(config)#iscsi enable
```

iscsi target port

Use the `iscsi target port` command in Global Configuration mode to configure iSCSI port(s), target addresses and names. To delete iSCSI port(s) or target ports, use the **no** form of this command.

Syntax

```
iscsi target port tcp-port-1 [tcp-port-2... tcp-port-16] [address ip-address]  
[name targetname]
```

```
no iscsi target port tcp-port-1 [tcp-port-2... tcp-port-16] [address ip-address]
```

Parameter Description

Parameter	Description
<i>tcp-port</i>	TCP port number or list of TCP port numbers on which iSCSI target(s) listen to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
<i>ip-address</i>	IP address of the iSCSI target. When the no form is used, and the <i>tcp port</i> to be deleted is one bound to a specific IP address, the address field must be present.

Parameter	Description
<i>targetname</i>	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator MUST present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection. The target name can consist of any printable character except for an exclamation point or a double quote as the first character. A question mark may not appear anywhere in the target name. The name can contain embedded blanks if enclosed in double quotes.

Default Configuration

iSCSI well-known ports 3260 and 860 are configured by default but can be removed as any other configured target.

Command Mode

Global Configuration mode.

User Guidelines

- When working with private iSCSI ports (not IANA assigned iSCSI ports 3260/860), it is recommended to specify the target IP address as well, so the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, AND their destination IP is the target's IP address. This way the CPU is not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these {un-reserved} ports).
- When a port is already defined and not bound to an IP address, and you want to bind the port to an IP address, first remove the port by using the **no** form of the command and then add it again, this time together with the relevant IP address.
- Target names are only for display when using the [show iscsi](#) command. These names are not used to match (or for doing any sanity check) with the iSCSI session information acquired by snooping.
- A maximum of 16 TCP ports can be configured either bound to IP or not.

Example

The following example configures TCP Port 49154 to target IP address 172.16.1.20.

```
console(config)#iscsi target port 49154 address  
172.16.1.20
```

show iscsi

Use the `show iscsi` command in Privileged EXEC mode to display the iSCSI configuration.

Syntax

```
show iscsi
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 enabled  
  
iSCSI vpt is 5
```

```
Session aging time: 10 min  
Maximum number of sessions is 192
```

```
-----  
iSCSI Targets and TCP Ports:  
-----
```

```
TCP Port      Target IP Address      Name  
860  --  
3260  --  
  
30001 172.16.1.1iqn.1993-11.com.disk-  
vendor:diskarrays.sn.45678.tape:sys1.xyz  
30033172.16.1.10
```

```
-----  
iSCSI Static Rule Table  
-----
```

```
Index TCP Port IP Address IP Address Mask  
TCP Port Target IP AddressName
```

show iscsi sessions

Use the `show iscsi sessions` command in Privileged EXEC mode to display the iSCSI status.

Syntax

```
show iscsi sessions [detailed]
```

- `detailed` — Displayed list has additional data when this option is used.

Default Configuration

If not specified, sessions are displayed in short mode (not detailed).

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

The following examples show summary and detailed information about the iSCSI sessions.

```
console#show iscsi sessions
```

```
Target: iqn.1993-11.com.disk-  
vendor:diskarrays.sn.45678
```

```
-----  
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
```

```
ISID: 11
```

```
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
```

```
ISID: 222
```

```
-----  
Target: iqn.103-1.com.storage-vendor:sn.43338.
```

```
storage.tape:sys1.xyz
```

```
Session 3:
```

```
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
```

```
Session 4:
```

```
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
```

```
Console# show iscsi sessions detailed
```

```
Target: iqn.1993-11.com.disk-  
vendor:diskarrays.sn.45678
```

```
-----  
Session 1:
```

```
Initiator: iqn.1992-04.com.os  
vendor.plan9:cdrom.12.storage:sys1.xyz
```


Time started: 17-Jul-2008 10:04:50

Time for aging out: 10 min

ISID: 11

Initiator Initiator Target Target

IP address TCP port IP address IP port

172.16.1.3 49154 172.16.1.20 30001

172.16.1.4 49155 172.16.1.21 30001

172.16.1.5 49156 172.16.1.22 30001

Session 2:

Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10

Time started: 17-Aug-2008 21:04:50

Time for aging out: 2 min

ISID: 22

Initiator Initiator Target Target

IP address TCP port IP address IP port

172.16.1.30 49200 172.16.1.20 30001

172.16.1.30 49201 172.16.1.21 30001

Link Dependency Commands

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.

Commands in this Chapter

This chapter explains the following commands:

<code>action</code>	<code>add port-channel</code>
<code>link-dependency group</code>	<code>depends-on</code>
<code>add gigabitethernet</code>	<code>show link-dependency</code>
<code>add tengigabitethernet</code>	—

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}
```

Parameter Description

Parameter	Description
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-dependency group

Use the **link-dependency group** command to enter the link-dependency mode to configure a link-dependency group.

Syntax

```
link-dependency group GroupId
```

```
no link-dependency 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-dependency group 1
console (config-linkDep-group-1) #
```

add gigabitethernet

Use this command to add member gigabit Ethernet port(s) to the dependency list.

Syntax

`add gigabitethernet intf-list`

- *intf-list* — List of Ethernet interfaces in unit/slot/port format. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console (config-depend-1) #add gigabitethernet 1/0/1
```

add tengigabitethernet

Use this command to add member ten gigabit Ethernet port(s) to the dependency list.

Syntax

`add tengigabitethernet intf-list`

- *intf-list* — List of Ethernet interfaces in unit/slot/port format. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-depend-1)#add tengigabitethernet 1/0/1
```

add port-channel

Use this command to add member port channels to the dependency list.

Syntax

`add port-channel intf-list`

`no add port-channel port channel list`

- *intf-list* — List of port-channel numbers. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate the range of port-channels. (Range: Valid port-channel list or range)
- *port-channel-list* — List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
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 {gigabitethernet | port-channel | tengigabitethernet |  
fortygigabitethernet} intf-list
```

```
no depends-on {gigabitethernet | port-channel | tengigabitethernet |  
fortygigabitethernet} intf-list
```

- *intf-list* — List of ports in unit/slot/port format or port-channel numbers. Separate nonconsecutive items with a comma and no spaces. Use a hyphen to designate the range of ports or port-channel numbers. (Range: Valid Ethernet interface or port-channel list or range)

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.

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]
```

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

No specific guidelines

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 UpGroup
```

```
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

The IEEE 802.1AB standard defines the Link Layer Discovery Protocol (LLDP). This protocol allows stations residing on an 802 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. PowerConnect 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 disabled 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 Chapter

This chapter explains the following commands:

<code>clear lldp remote-data</code>	<code>lldp receive</code>	–
<code>clear lldp statistics</code>	<code>lldp timers</code>	–
–	<code>lldp transmit</code>	–
–	<code>lldp transmit-mgmt</code>	–
–	<code>lldp transmit-tlv</code>	<code>show lldp remote-device</code>
–	<code>show lldp</code>	<code>show lldp statistics</code>
<code>lldp notification</code>	<code>show lldp interface</code>	–
<code>lldp notification-interval</code>	<code>show lldp local-device</code>	–

clear lldp remote-data

Use the `clear lldp remote-data` command in Privileged EXEC mode to delete all LLDP information from the remote data table.

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 in Privileged EXEC mode 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
```

Ildp 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-1/0/3)#lldp notification
```

Ildp 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 lldp 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-1/0/3)#lldp receive
```

Ildp 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 re-initialization. (Range: 1–10 seconds)

Default Configuration

The default transmit interval is 30 seconds.

The default hold-multiplier is 4.

The default delay before re-initialization 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 re-initialization.

```
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-1/0/3)#lldp transmit
```

Ildp transmit-mgmt

Use the **ildp transmit-mgmt** command in Interface Configuration mode to include transmission of the local system management address information in the LLDPDU. To cancel inclusion of the management information, use the **no** form of this command.

Syntax

```
ildp transmit-mgmt
```

```
no ildp transmit-mgmt
```

Default Configuration

By default, management address information is not included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to include management information in the LLDPDU.

```
console(config-if-1/0/3)#ildp transmit-mgmt
```

Ildp transmit-tlv

Use the **ildp transmit-tlv** command in Interface Configuration mode to specify which optional type-length-value settings (TLVs) in the 802.1AB basic management set will be transmitted in the LLDPDU. To remove an optional TLV, use the **no** form of this command.

Syntax

```
ildp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
```

```
no ildp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
```

- `sys-name` — Transmits the system name TLV
- `sys-desc` — Transmits the system description TLV
- `sys-cap` — Transmits the system capabilities TLV
- `port desc` — Transmits the port description TLV

Default Configuration

By default, no optional TLVs are included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to include the system description TLV in local data transmit.

```
console(config-if-1/0/3)#lldp transmit-tlv sys-desc
```

show lldp

Use the `show lldp` command in Privileged EXEC mode to display the current LLDP configuration summary.

Syntax

```
show lldp
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the current LLDP configuration summary.

```
console# show lldp
```

```
Global Configurations:
```

```
Transmit Interval: 30 seconds
```

```
Transmit TTL Value: 120 seconds
```

```
Reinit Delay: 2 seconds
```

```
Notification Interval: limited to every 5 seconds
```

```
console#show lldp
```

```
LLDP transmit and receive disabled on all interfaces
```

show lldp interface

Use the `show lldp interface` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
Interface Link Transmit Receive Notify TLVs Mgmt
-----
-
1/0/1      Up    Enabled Enabled Enabled 0,1,2,3 Y
1/0/2      Down Enabled Enabled Disabled Y
1/0/3      Down Disabled Disabled Disabled 1,2 N
TLV Codes: 0 - Port Description, 1 - System Name, 2 -
System Description, 3 -
System Capability
```

```
console# show lldp interface 1/0/1
Interface Link Transmit Receive Notify TLVs Mgmt
-----
-
1/0/1      Up    Enabled Enabled Enabled 0,1,2,3 Y
TLV Codes: 0 - Port Description, 1 - System Name, 2 -
System Description, 3 - System Capability
```

show lldp local-device

Use the **show lldp local-device** command in Privileged EXEC mode 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 remote data.
- *interface* — Specifies a valid physical 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, Config mode and all Config sub-modes

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
1/0/1	00:62:48:00:00:02	

```
console# show lldp local-device detail 1/0/1
```

```
LLDP Local Device Detail
```

```
Interface: 1/0/1
```

```
Chassis ID Subtype: MAC Address
```

```
Chassis ID: 00:62:48:00:00:00
```

```
Port ID Subtype: MAC Address
```

```
Port ID: 00:62:48:00:00:02
```

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 remote-device

Use the `lldp remote-device` command in Privileged EXEC mode 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 physical interface on the device. Substitute `gigabitethernet unit/slot/port` or `tengigabitethernet unit/slot/port` or `fortygigabitethernet unit/slot/port`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

These examples show current LLDP remote data, including a detailed version.

```
console#show lldp remote-device
```

```
Local Remote
```

Interface	Device	ID	Port	ID	TTL
-----	-----	-----	-----	-----	-----
1/0/1	01:23:45:67:89:AB	01:23:45:67:89:AC	60		seconds
1/0/2	01:23:45:67:89:CD	01:23:45:67:89:CE	120		seconds
1/0/3	01:23:45:67:89:EF	01:23:45:67:89:FG	80		seconds

```
console# show lldp remote-device detail 1/0/1
```

```
Ethernet1/0/1,
```

```
Remote ID: 01:23:45:67:89:AB
```

```
System Name: system-1
```

```
System Description:
```

```
System Capabilities: Bridge
```

```
Port ID: 01:23:45:67:89:AC
```

```
Port Description: 1/0/4
```

```
Management Address: 192.168.112.1
```

```
TTL: 60 seconds
```


show lldp statistics

Use the `show lldp statistics` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following examples shows an example of the display of current LLDP traffic statistics.

```
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

```

          Tx   Rx                TLV   TLV
TLV  TLV   TLV
Interface Total Total Discards Errors Ageout Discards
Unknowns MED  802.1 802.3
-----
1/0/11      29395 82562 0      0      1      0      0
0      1      4

```

The following table explains the fields in this example.

Fields	Description
Last Update	The value of system of time the last time a remote data entry was created, modified, or deleted.
Total Inserts	The number of times a complete set of information advertised by a remote device has been inserted into the table.
Total Deletes	The number of times a complete set of information advertised by a remote device has been deleted from the table.
Total Drops	Number of times a complete set of information advertised by a remote device could not be inserted due to insufficient resources.
Total Ageouts	Number of times any remote data entry has been deleted due to time-to-live (TTL) expiration.
Transmit Total	Total number of LLDP frames transmitted on the indicated port.
Receive Total	Total number of valid LLDP frames received on the indicated port.

Fields	Description
Discards	Number of LLDP frames received on the indicated port and discarded for any reason.
Errors	Number of non-valid LLDP frames received on the indicated port.
Ageouts	Number of times a remote data entry on the indicated port has been deleted due to TTL expiration.
TLV Discards	Number LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.
TLV Unknowns	Number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.
TLV MED	Number of OUI specific MED (Media Endpoint Device) TLVs received.
TLV 802.1	Number of OUI specific 802.1 specific TLVs received.
TLV 802.3	Number of OUI specific 802.3 specific TLVs received.

Multicast VLAN Registration Commands

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 Chapter

This chapter explains the following commands:

<code>mvr</code>	<code>mvr type</code>
<code>mvr group</code>	<code>mvr vlan group</code>
<code>mvr mode</code>	<code>show mvr</code>
<code>mvr querytime</code>	<code>show mvr members</code>
<code>mvr vlan</code>	<code>show mvr interface</code>
<code>mvr immediate</code>	<code>show mvr traffic</code>

mvr

Use the `mvr` command in Global Config and Interface Config modes to enable MVR. Use the `no` form of this command to disable MVR.

Syntax

`mvr`

`no mvr`

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is `Disabled`.

Command Mode

Global Config, Interface Config

User Guidelines

MVR can only be configured on physical interfaces.

mvr group

Use the **mvr group** command in Global Config 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]
```

```
no mvr group A.B.C.D [count]
```

Parameter Description

Parameter	Description
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 Config

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	<ul style="list-style-type: none">• Not an IP multicast group address• Illegal IP multicast group address

Example

```
console (config) #mvr
```

```
console(config)#mvr group 239.0.1.0 100
console(config)#mvr vlan 10
```

mvr mode

Use the **mvr mode** command in Global Config 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
```

Parameter Description

Parameter	Description
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 Config

User Guidelines

This command has no user guidelines.

mvr querytime

Use the **mvr querytime** command in Global Config mode to set the MVR query response time. 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`

Parameter Description

Parameter	Description
querytime	The query time is a maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time only applies to receiver ports. The query time is specified in tenths of a second.

Default Configuration

The default value is 5 tenths of a second.

Command Mode

Global Config

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	Defaulting MVR query response time.
Error Completion Message	None

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 mode dynamic
console(config-if-Gi1/0/1)#mvr querytime 10
```

mvr vlan

Use the **mvr vlan** command in Global Config 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 *1-4094*

no mvr vlan

Parameter Description

Parameter	Description
vlan	The VLAN 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 Config

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	MVR multicast VLAN ID is set to the default value which is equal to 1.
Error Completion Message	Receiver port in mVLAN, operation failed.

mvr immediate

Use the **mvr immediate** command in Interface Config 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`

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is **Disabled**.

Command Mode

Interface Config

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 mode dynamic
console(config-if-Gi1/0/1)#mvr immediate
```

mvr type

Use the `mvr type` command in Interface Config mode to set the MVR port type. Use the `no` form of this command to set the MVR port type to **None**.

Syntax

`mvr type {receiver | source}`

`no mvr type`

Parameter Description

Parameter	Description
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 Config

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	<ul style="list-style-type: none">• Port is a Trunk port, operation failed.• Receiver port in mVLAN, operation failed.

Example

```
console (config) #mvr
console (config) #mvr group 239.1.1.1
console (config) #exit
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)#interface Gi1/0/24
console(config-if-Gi1/0/24)#switchport mode trunk
console(config-if-Gi1/0/24)#switchport trunk native
vlan 99
console(config-if-Gi1/0/24)#switchport trunk allowed
vlan add 99
console(config-if-Gi1/0/24)#mvr
console(config-if-Gi1/0/24)#mvr type source
console(config-if-Gi1/0/24)#exit

```

mvr vlan group

Use the **mvr vlan group** command in Interface Config 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 mVLANgroup A.B.C.D
no mvr vlan mVLANgroup A.B.C.D

```

Parameter Description

Parameter	Description
VLAN	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 Config

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-if-Gi1/0/1)#interface Te1/1/1
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 in Privileged EXEC mode to display global MVR settings.

Syntax

```
show mvr
```

Parameter Description

The following table explains the output parameters.

Parameter	Description
MVR Running	MVR running state. It can be enabled or disabled.
MVR Multicast VLAN	Current MVR multicast VLAN. It can be in the range from 1 to 4094.
MVR Max Multicast Groups	The maximum number of multicast groups that is supported by MVR.
MVR Current Multicast groups	The current number of MVR groups allocated.
MVR Query Response Time	The current MVR query response time.
MVR Mode	The current MVR mode. It can be compatible or dynamic.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	MVR disabled

Example

```

console #show mvr
MVR Running..... TRUE
MVR multicast VLAN..... 1200
MVR Max Multicast Groups..... 256

```

```

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 in Privileged EXEC mode to display the MVR membership groups allocated.

Syntax

```
show mvr members [A.B.C.D]
```

Parameter Description

The parameter is a valid multicast address in IPv4 dotted notation. The following table explains the output parameters.

Parameter	Description
MVR Group IP	MVR group multicast IP address.
Status	The status of the specific MVR group. It can be active or inactive.
Members	The list of ports which participates in the specific MVR group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	MVR disabled

Examples

```
console#show mvr members
```

```
MVR Group IP          Status          Members
-----
224.1.1.1             INACTIVE       1/0/1, 1/0/2,
1/0/3
```

```
console#show mvr members 224.1.1.1
```

```
MVR Group IP          Status          Members
-----
224.1.1.1             INACTIVE       1/0/1, 1/0/2,
1/0/3
```

show mvr interface

Use the `show mvr interface` command in Privileged EXEC mode to display the MVR enabled interfaces configuration.

Syntax

```
show mvr interface [interface-id [members [vlan vid]]]
```

Parameter Description

Parameter	Description
Interface-id	Identifies a specific interface.

Parameter	Description
VID	VLAN identifier.

The following table explains the output parameters.

Parameter	Description
Port	Interface number
Type	The MVR port type. It can be None , Receiver , or Source type.
Status	The interface status. It consists of two characteristics: 1 active or inactive indicating if port is forwarding. 2 inVLAN or notInVLAN indicating if the port is part of any VLAN
Immediate Leave	The state of immediate mode. It can be enabled or disabled .

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	MVR disabled

Examples

```
console#show mvr interface
```

Port	Type	Status
Immediate Leave		
-----	-----	-----
-----	-----	-----
1/0/9	RECEIVER	ACTIVE/inVLAN
DISABLED		

```
console#show mvr interface 1/0/9
```

```
Type: RECEIVER Status: ACTIVE Immediate Leave:
DISABLED
```

```
console#show mvr interface Fa1/0/23 members
```

```
235.0.0.1 STATIC ACTIVE
```

```
console#show mvr interface Fa1/0/23 members vlan 12
```

```
235.0.0.1 STATIC ACTIVE
```

```
235.1.1.1 STATIC ACTIVE
```

show mvr traffic

Use the **show mvr traffic** command in Privileged EXEC mode to display global MVR statistics.

Syntax

```
show mvr traffic
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	None
Error Completion Message	MVR disabled

Examples

The following table explains the output parameters.

Parameter	Description
IGMP Query Received	Number of received IGMP Queries.
IGMP Report V1 Received	Number of received IGMP Reports V1.
IGMP Report V2 Received	Number of received IGMP Reports V2.
IGMP Leave Received	Number of received IGMP Leaves.
IGMP Query Transmitted	Number of transmitted IGMP Queries.
IGMP Report V1 Transmitted	Number of transmitted IGMP Reports V1.
IGMP Report V2 Transmitted	Number of transmitted IGMP Reports V2.
IGMP Leave Transmitted	Number of transmitted IGMP Leaves.
IGMP Packet Receive Failures	Number of failures on receiving the IGMP packets.
IGMP Packet Transmit Failures	Number of failures on transmitting the IGMP packets.

```
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

Port Channel Commands

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.

In the PowerConnect system, the Actor System waits for 3 seconds before aggregating manually. The 3 second wait time is specified by the protocol standard.

If a manual 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 no different from a dynamically configured LAG. All the requirements for the member ports hold true (member ports must be physical, 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.

A static LAG does not transmit or process received LACPDU's, that is, the member ports do not transmit LACPDU's and all the LACPDU's it may receive are dropped. A dropped counter is maintained to count the number of such PDU's.

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 members are added to a LAG, they are removed from all existing VLAN membership. When members are removed from a LAG, the members rejoin the VLANs that they were previously members of as per the configuration file.

The LAG interface can be a member of a VLAN complying with IEEE 802.1Q.

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.

Port Channels

Trunking, which is also called Port Channels or Link Aggregation, is initiated and maintained by the periodic exchanges of Link Aggregation Control PDUs (LACPDU)s. When LACP is enabled for a physical interface, LACPDU)s must not be dropped for any reason. Conversely, when LACP is disabled for the physical interface LACPDU)s must be dropped.

From a system perspective, a LAG is treated as a physical port. A LAG and a physical port use the same configuration parameters for administrative enable/disable, port priority, and path cost. When a physical port is configured as part of a LAG, it no longer participates in forwarding operations until the LAG becomes active.

A LAG failure of one or more of the links does not stop traffic in any manner. Upon failure, the flows mapped to a link are dynamically reassigned to the remaining links of the LAG. Similarly when links are added to a LAG, the conversations may need to be shifted to a new link.

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 physical port within port channel for transmitting the packet to keep original packets order.

The hashing algorithm is configurable for each LAG. The types of LAG algorithms available may vary depending upon platform capabilities. 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.

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 a physical port within the port channel for transmitting the packet to keep original packets 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

PowerConnect 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.

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.

As part of Release 4.0, the LAG hashing support is extended to support 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.

Manual Aggregation of LAGs

PowerConnect switching supports the manual addition and deletion of links to aggregates.

In the manual configuration of aggregates, the ports send their Actor Information (LACPDU)s to the partner system in order to find a suitable Partner to form an aggregation. When the Partner System neglects to respond using LACPDU,s the PowerConnect switching aggregates manually. The PowerConnect switching uses the currently configured default Partner Values for Partner Information.

Manual Aggregation of LAGs

PowerConnect switching supports the manual addition and deletion of links to aggregates.

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.

Commands in this Chapter

This chapter explains the following commands:

<code>channel-group</code>	<code>lacp system-priority</code>
<code>interface port-channel</code>	<code>lacp timeout</code>
<code>interface range port-channel</code>	–
<code>hashing-mode</code>	<code>port-channel local-preference</code>
–	<code>port-channel min-links</code>
–	<code>show interfaces port-channel</code>
<code>lacp port-priority</code>	<code>show lacp</code>
–	<code>show statistics port-channel</code>

channel-group

Use the **channel-group** command in Interface 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 1/0/5 is configured to port-channel 1 without LACP (static LAG).

```
console(config)# interface gigabitethernet 1/0/5
console(config-if-1/0/5)# channel-group 1 mode on
```

The following example shows how port 1/0/6 is configured to port-channel 1 with LACP (dynamic LAG).

```
console(config)# interface gigabitethernet 1/0/6
console(config-if-1/0/6)# channel-group 1 mode active
```

interface port-channel

Use the `interface port-channel` command in Global Configuration mode to configure a port-channel type and 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

This command has no user guidelines.

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.

```
console(config)# interface range port-channel 1-2,8
console(config-if)#
```

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 (3).

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

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (port-channel)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface port-channel 1
console(config-if-po1)#hashing-mode 4
console(config-if-po1)#no hashing mode
```

lACP port-priority

Use the **lACP port-priority** command in Interface Configuration mode 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

User Guidelines

This command has no user guidelines.

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-1/0/8)#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* — Port priority value. (Range: 1–65535)

Default Configuration

The default system priority value is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the system priority to 120.

```
console(config)#lacp system-priority 120
```


lacp timeout

Use the **lacp timeout** command in Interface Configuration mode to assign an administrative LACP timeout. To reset the default administrative LACP timeout, 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

User Guidelines

This command has no user guidelines.

Example

The following example assigns an administrative LACP timeout for port 1/0/8 to a long timeout value.

```
console(config)#interface gigabitethernet 1/0/8
console(config-if-1/0/8)#lacp timeout long
```

port-channel local-preference

Use the **port-channel local-preference** command in Interface Config 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 Config (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.

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

Parameter Description

Parameter	Description
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

This command has no default configuration.

Command Mode

Interface Configuration (port-channel) mode

User Guidelines

This command has no user guidelines.

show interfaces port-channel

Use the `show interfaces port-channel` command to show port-channel information.

Syntax Description

`show interfaces port-channel [port-channel-number]`

Parameter Description

The command displays the following information.

Parameter	Description
[<i>index</i>]	Number of the port channel to show. This parameter is optional. If the port channel number is not given, all the channel groups are displayed. (Range: Valid port-channel number, 1 to 48).
Local Prf	An additional field added to support the display of the local preference.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example #1

```
console#show interfaces port-channel
ChannelPorts  ChTypeHash Algorithm Typemin-Links
-----
-----
Po1Inactive: Gi1/0/3Dynamic31
Po2No Configured PortsStatic31
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
```

Example #2

```
console#show interfaces port-channel 1
```

```
Channel   Ports                               Ch-Type   Hash Type Min-links
Local Prf
-----
--
Po1       Inactive: Gi1/0/1, Gi1/0/2,        Dynamic   3         1
Enabled
          Gi1/0/3, Gi1/0/4
```

show lacp

Use this command in Privileged EXEC mode to display LACP information for Ethernet ports.

Syntax

```
show lacp {gigabitethernet unit/slot/port | port-channel port-channel-number
| tengigabitethernet unit/slot/port / fortygigabitethernet unit/slot/port
[{parameters | statistics}]
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display LACP Ethernet interface information.

```
console#show lacp gigabitethernet 1/0/1
```

Port 1/0/1 LACP parameters:

Actor

system priority:	1
system mac addr:	00:00:12:34:56:78
port Admin key:	30
port Oper key:	30
port Oper priority:	1
port Admin timeout:	LONG
port Oper timeout:	LONG
LACP Activity:	ACTIVE
Aggregation:	AGGREGATABLE
synchronization:	FALSE
collecting:	FALSE
distributing:	FALSE
expired:	FALSE

Partner

system priority:	0
system mac addr:	00:00:00:00:00:00
port Admin key:	0
port Oper key:	0
port Admin priority:	0
port Oper priority:	0

port Oper timeout:	LONG
LACP Activity:	ASSIVE
Aggregation:	AGGREGATABLE
synchronization:	FALSE
collecting:	FALSE
distributing:	FALSE
expired:	FALSE
Port 1/0/1 LACP Statistics:	
LACP PDUs sent:	2
LACP PDUs received:	2

show statistics port-channel

Use the `show statistics port-channel` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 1064
Packets RX and TX 65-127 Octets..... 140
Packets RX and TX 128-255 Octets..... 201
Packets RX and TX 256-511 Octets..... 418
Packets RX and TX 512-1023 Octets..... 1
Packets RX and TX 1024-1518 Octets..... 0
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Total Packets Received with MAC Errors..... 0
Jabbers Received..... 0
Fragments/Undersize Received..... 0
Alignment Errors..... 0
--More-- or (q)uit
FCS Errors..... 0
Overruns..... 0
```



```

Total Received Packets Not Forwarded..... 0
Local Traffic Frames..... 0
802.3x Pause Frames Received..... 0
Unacceptable Frame Type..... 0
Multicast Tree Viable Discards..... 0
Reserved Address Discards..... 0
Broadcast Storm Recovery..... 0
CFI Discards..... 0
Upstream Threshold..... 0
Total Packets Transmitted (Octets).....
263567
Max Frame Size..... 1518
Total Packets Transmitted Successfully..... 1824
Unicast Packets Transmitted..... 330
Multicast Packets Transmitted..... 737
Broadcast Packets Transmitted..... 757
Total Transmit Errors..... 0
FCS Errors..... 0
--More-- or (q)uit
Tx Oversized..... 0
Underrun Errors..... 0
Total Transmit Packets Discarded..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0
Port Membership Discards..... 0

```

```
802.3x Pause Frames Transmitted..... 0
GVRP PDUs received..... 0
GVRP PDUs Transmitted..... 0
GVRP Failed Registrations..... 0
Time Since Counters Last Cleared..... 0 day
0 hr 17 min 52 sec
console#
```

Port Monitor Commands

PowerConnect 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 single probe session. A session consists of one destination port and 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.

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 port. The probe port does not forward any traffic and does not receive any traffic. The probe tool attached to the probe port is generally unable to ping the networking device or ping through the networking device, and nobody is able to ping the probe tool.

Commands in this Chapter

This chapter explains the following commands:

monitor session

Use the **monitor session** command in Global Configuration mode to configure a probe port and a monitored port for monitor session (port monitoring). Use the `src-interface` 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 | tx}` option, the destination port monitors both ingress and egress packets. Use the destination interface to specify the interface to receive the monitored traffic. Use the `mode` parameter to enable the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Use the **no** form of the command to remove the monitoring session.

Syntax

```
monitor session session_number {source interface interface-id [rx | tx] |  
destination interface interface-id}
```

no monitor session

- *session_number*— Session identification number.
- **interface-id** — Ethernet interface (Range: Any valid Ethernet Port), CPU interface. CPU interface is not supported as a destination interface.
- **rx** — Monitors received packets only. If no option specified, monitors both rx and tx.
- **tx** — Monitors transmitted packets only. If no option is specified, monitors both rx and tx.
- Use the **mode** keyword to enable the session monitoring.

Default Configuration

Monitor sessions are not enabled by default.

Command Mode

Global Configuration mode

User Guidelines

The source of a monitoring session must be configured before the destination can be configured. Only one session with a single destination is supported, however, that session supports multiple sources.

Example

The following examples show a simple port level configuration that mirrors both transmitted and received packet from one port to another.

```
console(config)#monitor session 1 source interface
tel/0/8
```

```
console(config)#monitor session 1 destination
interface tel/0/10
```

```
console(config)#monitor session 1 mode
```

show monitor session

Use the **show monitor session** command in Privileged EXEC mode to display status of port monitoring.

Syntax

```
show monitor session session_number
```

- *session_number*— Session identification number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following examples shows port monitoring status.

```
console#show monitor session 1
```

Session ID Port	Type	Admin Mode	Probe Port	Mirrored
1	Rx, Tx	Enable	1/0/10	1/0/8

QoS Commands

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 PowerConnect 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 a physical port 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 IP access lists, both standard and extended. 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 PowerConnect CoS Queueing feature allows the user to directly configure device queueing 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 PowerConnect 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, IP precedence, or IP DSCP contents of a packet. If none of these fields are 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:

- 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 nonIP packet arrives at a port configured to trust the IP precedence or IP DSCP value.

Commands in this Chapter

This chapter explains the following commands:

assign-queue	mark cos	match ip tos	show class-map
class	mark ip-dscp	match protocol	show classofservice dot1p-mapping
class-map	mark ip-precedence	match source-address mac	show classofservice ip-dscp-mapping
class-map rename	match class-map	match srcip	show classofservice trust
classofservice dot1p-mapping	match cos	match srcip6	show diffserv
classofservice ip-dscp-mapping	match destination-address mac	match src4port	show diffserv service interface
classofservice trust	match dstip	match vlan	show diffserv service interface port-channel
conform-color	match dstip6	mirror	show diffserv service brief
cos-queue min-bandwidth	match dst4port	police-simple	show interfaces cos-queue
cos-queue random-detect	match ethertype	policy-map	show interfaces random-detect
cos-queue strict	match ip6flowlbl	random-detect queue-parms	show policy-map
diffserv	match ip dscp	random-detect exponential-weighting-constant	show policy-map interface
drop	match ip precedence	redirect	show service-policy
–	–	service-policy	traffic-shape

assign-queue

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

This command has no user guidelines.

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) #policy-map DELL1
console (config-classmap) #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 the existing class, use the **no** form of this command.

Syntax

```
class-map match-all class-map-name [{ipv4 | ipv6}]
```

```
no class-map match-all class-map-name
```

- *class-map-name* — a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Default Configuration

The class-map defaults to ipv4.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example creates a class-map named "DELL" which requires all ACE's to be matched.

```
console (config) #class-map DELL
console (config-cmap) #
```

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 802.1p 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 802.1ppriority trafficclass
```

```
no classofservice dot1p-mapping
```

- *802.1ppriority*— 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 dot1p mapping is as follows:

User Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Command Mode

Global Configuration or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

None

Example

The following example configures mapping for user priority 1 and traffic class 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
```

Parameter Description

Parameter	Description
<i>ipdscp</i>	Specifies the IP DSCP value to which you map 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).
<i>trafficclass</i>	Specifies the traffic class for this value mapping. (Range: 0–6).

Default Configuration

The default DSCP mapping is as follows:

IP DSCP	Traffic Class
0(be/cs0)	1
1	1

IP DSCP	Traffic Class
2	1
3	1
4	1
5	1
6	1
7	1
8(cs1)	0
9	0
10(af11)	0
11	0
12(af12)	0
13	0
14(af13)	0
15	0
16(cs2)	0
17	0
18(af21)	0
19	0
20(af22)	0
21	0
22(af23)	0
23	0
24(cs3)	1
25	1
26(af31)	1
27	1
28(af32)	1
29	1

IP DSCP	Traffic Class
30(af33)	1
31	1
32(cs4)	2
33	2
34(af41)	2
35	2
36(af42)	2
37	2
38(af43)	2
39	2
40(cs5)	2
41	2
42	2
43	2
44	2
45	2
46(ef)	2
47	2
48(cs6)	3
49	3
50	3
51	3
52	3
53	3
54	3
55	3
56(cs7)	3
57	3

IP DSCP	Traffic Class
58	3
59	3
60	3
61	3
62	3
63	3

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays mapping for IP DSCP 1 and traffic class 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 untrusted, 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 dot1p (802.1p) packet markings.
- **untrusted** — Sets the Class of Service Trust Mode for all interfaces to Untrusted.

- `ip-dscp` — Specifies that the mode be set to trust IP DSCP packet markings.

Default Configuration

This command has no default configuration.

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 displays how you set the class of service trust mode of an interface to trust dot1p (802.1p) packet markings when in Global Configuration mode.

```
console(config)#classofservice trust dot1p
```

The following example displays how you set the class of service trust mode of an interface to trust IP Precedence packet mark

```
console(config)#classofservice trust ip-precedence
```

conform-color

Use the `conform-color` command in Policy-Class-Map Configuration mode to specify second-level matching for traffic flow, the only possible actions are `drop`, `setdscp-transmit`, `set-prec-transmit`, or `transmit`. In this two-rate form of the policy command, the conform action defaults to `send`, the exceed action defaults to `drop`, and the violate action defaults to `drop`. These actions can be set with this command.

Syntax

```
conform-color
```

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 the **conform-color** command.

```
console (config-policy-classmap) #conform-color
test_class (test_class is <class-map-name>
```

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 for an interface. You can specify as many bandwidths as there are interfaces (*bw-0* through *bw-n*). (Range: 0–100 in increments of 5)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

The maximum number of queues supported per interface is seven. When ETS is operational on a 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 for seven interfaces.

```
console (config) #cos-queue min-bandwidth 0 0 5 5 10 10 10
```

cos-queue random-detect

Use the `cos-queue random-detect` command in Global Configuration or Interface Configuration mode to configure 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.

Syntax

```
cos-queue {random-detect queue-id1 [queue-id2..queue-idn]}  
no cos-queue {random-detect queue-id1 [queue-id2..queue-idn]}
```

Parameter Description

Parameter	Description
queue-id	An integer indicating the 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.

Command Mode

Interface Configuration (physical or port-channel) 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.

This command can be used in Interface Range mode.

Use the [cos-queue min-bandwidth](#) command to configure the minimum bandwidth percentage for the CoS queues.

Use the [show interfaces random-detect](#) command to display the WRED configuration.

Example

Enable WRED on the default CoS queue for unmarked packets and set the green, yellow, red and non-TCP packet thresholds to utilize WRED at 98% of port bandwidth with a drop probability of 1%.

```
console(config)# cos-queue random-detect 1
console(config)# random-detect queue-params 1 min-
thresh 98 98 98 98 max-thresh 100 100 100 100 drop-
prob-scale 1 1 1 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 each specified queue. To restore the default weighted scheduler mode for each specified queue, use the `no` form of this command.

Syntax

```
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

This command has no user guidelines.

Example

The following example displays how to activate the strict priority scheduler mode for two queues.

```
console(config)#cos-queue strict 1 2
```

The following example displays how to activate the strict priority scheduler mode for three queues.

```
console(config)#cos-queue strict 1 2 4
```

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 activated. When enabled, DiffServ services are activated. To set the DiffServ operational mode to inactive, use the **no** form of this command.

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.

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 priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

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

This command has no user guidelines.

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.

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

This command has no user guidelines.

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.

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.

This command has no user guidelines.

Example

The following example displays

```
console (config) #policy-map p1 in
console (config-policy-map) #class c1
console (config-policy-classmap) #mark ip-precedence 2
console (config-policy-classmap) #
```

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.

Syntax

```
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.

- 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 reclass 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(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(config-classmap)#no match class-map Dell
```

match cos

Use the **match cos** command in Class-Map Configuration mode to add to the specified class definition 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).

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 to the specified class definition a match condition based on the destination MAC address of a packet.

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 displays adding a match condition for the specified MAC address and bit mask.

```
console(config-classmap)#match destination-address  
mac AA:ED:DB:21:11:06 FF:FF:FF:EF:EE:EE
```

match dstip

Use the **match dstip** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination IP address of a packet.

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  
10.240.0.0
```

match dstip6

The **match dstip6** command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

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::/32
```

match dstl4port

Use the **match dstl4port** command in Class-Map Configuration mode to add 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.

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 to the specified class definition a match condition based on the value of the ethertype.

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**, **mplsmcast**, **mplsucast**, **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.

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. This 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.

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

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.

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.

Syntax

`match 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 add 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.

Syntax

`match protocol {protocol-name | protocol-number}`

- *protocol-name* — Specifies one of the supported protocol name keywords. The supported values are *icmp*, *igmp*, *ip*, *tcp*, and *udp*.
- *protocol-number* — Specifies the standard value assigned by IANA. (Range 0–255)

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 "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.

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.

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.

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::/32
```

match src14port

Use the **match src14port** 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.

Syntax

`match srcl4port {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.

Syntax

`match vlan vlan-id`

- *vlan-id* — Specifies a VLAN ID as an integer. (Range: 0–4095)

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.

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 1/0/5.

```
console(config-policy-classmap)#mirror 1/0/5
```

police-simple

Use the **police-simple** command in Policy-Class-Map Configuration mode to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform.

Syntax

```
police-simple {datarate burstsize conform-action {drop | set-pretransmit cos | set-dscp-transmit dscpval | transmit} [violateaction {drop | set-cos-transmit cos | set-prec-transmit cos | set-dscp-transmit dscpval | transmit}]}
```

- *datarate* — Data rate in kilobits per second (kbps). (Range: 1–4294967295)
- *burstsize* — Burst size in Kbps (Range: 1–128)
- **conform action** — Indicates what happens when the packet is conforming to the policing rule: it could be dropped, it could have its COS modified, it could have its IP precedence modified, or it could have its DSCP modified. The same actions are available for packets that do not conform to the policing rule.
- *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

Only one style of police command (simple) is allowed for a given class instance in a particular policy.

Example

The following example shows how to establish the traffic policing style for the specified class.

```
console(config-policy-classmap)#police-simple 33 34  
conform-action transmit violate-action transmit
```

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.

Syntax

```
policy-map policyname [in | out]  
no policy-map policyname
```

Parameter Description

Parameter	Description
<i>policyname</i>	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 green, yellow and red TCP and non-TCP packet minimum and maximum thresholds and corresponding drop probabilities on an interface or all interfaces.

Syntax

```
random-detect queue-parms queue-id [queue-id] ... min-thresh minthresh-green minthresh-yellow minthresh-red minthresh-nontcp max-thresh maxthresh-green maxthresh-yellow maxthresh-red maxthresh-nontcp
```

```
no random-detect queue-parms queue-id [queue-id] ...
```

Parameter Description

Parameter	Description
queue-id	The class of service queue. Range 0 to 6.
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 100.

Parameter	Description
max-thresh	The maximum threshold to ene dropping at the configured maximum drop probability for each color and for non-TCP packets. Range 0 to 100.
drop-prob-scale	The maximum drop probability. Range 0-100. Should be configured to be equal to or larger than the minimum probability.

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.

Queue ID	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
0	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
1	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
2	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
3	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
4	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
5	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10
6	40/30/20/100	100/ 90/ 80/100	10/ 10/ 10/ 10

Command Mode

Global Config mode, Interface Config mode (physical and port-channel), Interface Range mode

User Guidelines

The Green/Yellow/Red Ranges may overlap and are applied independently from each other. Within a color, the range from minimum to maximum is divided into eight (0...7) fixed rates at which packets are dropped based on the instantaneous egress queue size:

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

Packets are dropped at 100% when the queue size exceeds the maximum value and at 0% when the queue size is below the minimum value.

If the maxthresh is less than the corresponding minthresh, it is adjusted to be the minthresh plus one.

Example

This example configures interface te2/0/1 to drop packets queued for egress on the all interfaces (global config) or a single interface (interface config) with a piecewise linear approximation of the configured probability when the average queue size is within the given range:

- TCP Green Range: 15 to 74% - 10% maximum drop probability
- TCP Yellow Range: 75% to 89% - 50% maximum drop probability
- TCP Red Range: 90% to 98% - 75% maximum drop probability
- Non-TCP traffic: 50 to 98% - 50% maximum drop probability

```
console(config-if-Te2/0/1)#random-detect queue-parms 0 min-thresh 15 75 90 50 max-thresh 74 89 98 98 drop-prob-scale 10 50 75 50
```

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.

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 0.

Command Mode

Global Config mode, Interface Config mode (physical and port-channel), Interface Range mode

User Guidelines

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.

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).

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 1/0/1.

```
console(config-policy-classmap)#redirect 1/0/1
```

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.

Syntax

```
service-policy {in|out} policyname
```

```
no service-policy {in|out} policyname
```

Parameter Description

Parameter	Description
<i>policyname</i>	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

This command has no default configuration.

Command Mode

Global Configuration mode (for all system interfaces)

Interface Configuration (Ethernet, Port-channel) mode (for a specific interface)

User Guidelines

This command effectively enables DiffServ on an 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 catch the direction given for the policy map.

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. ACLs and DiffServ policies may not both exist on the same interface in the same direction.

Example

The following example shows how to attach a service policy named "DELL" to all interfaces.

```
console(config)#service-policy DELL
```

show class-map

Use the `show class-map` command in Privileged EXEC mode to display all configuration information for the specified class.

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, Config mode and all Config sub-modes

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
```

		Class L3	
Class Name		Type	Proto
Reference Class Name			

ipv4		All	ipv4
ipv6		All	ipv6
stop_http_class		All	ipv6
match_icmp6		All	ipv6

```
console#show class-map ipv4
```

```
Class Name..... ipv4
Class Type..... All
Class Layer3 Protocol..... ipv4
```

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..... All  
Class Layer3 Protocol..... ipv6
```

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 in Privileged EXEC mode to display the current Dot1p (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

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

If the interface is specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Example

The following example displays the dot1p traffic class mapping and user priorities.

```
console#show classofservice dot1p-mapping
```

User Priority	Traffic Class
0	1
1	1
2	6
3	4
4	3
5	4
6	5
7	6

The following table lists the parameters in the example and gives a description of each.

Parameter	Description
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

Use the `show classofservice ip-dscp-mapping` command in Privileged EXEC mode to display the current IP DSCP mapping to internal traffic classes for a specific interface.

Syntax

`show classofservice ip-dscp-mapping`

- Command is supported only globally.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Example

```
console#show classofservice ip-dscp-mapping
```

IP DSCP	Traffic Class
-----	-----
0 (be/cs0)	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1

8 (cs1)	0
9	0
10 (af11)	0
11	0
12 (af12)	0
13	0
14 (af13)	0
15	0
16 (cs2)	0
17	0
18 (af21)	0
19	0
--More-- or (q)uit	
20 (af22)	0
21	0
22 (af23)	0
23	0
24 (cs3)	1
25	1
26 (af31)	1
27	1
28 (af32)	1
29	1
30 (af33)	1
31	1
32 (cs4)	2

33	2
34 (af41)	2
35	2
36 (af42)	2
37	2
38 (af43)	2
39	2
40 (cs5)	2
41	2
42	2
--More-- or (q)uit	
43	2
44	2
45	2
46 (ef)	2
47	2
48 (cs6)	3
49	3
50	3
51	3
52	3
53	3
54	3
55	3
56 (cs7)	3
57	3

58	3
59	3
60	3
61	3
62	3
63	3

console#

show classofservice trust

Use the `show classofservice trust` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 1/0/2
Class of Service Trust Mode: Dot1P
```


show diffserv

Use the **show diffserv** command in Privileged EXEC mode to display the DiffServ general information, which includes the current administrative mode setting as well as the current and maximum number of DiffServ components.

Syntax

```
show diffserv
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display policy service information for the specified interface.

Syntax

```
show diffserv service interface {gigabitethernet unit/slot/port |  
tengigabitethernet unit/slot/port / fortygigabitethernet unit/slot/port}  
{in|out}
```

Parameter Description

Parameter	Description
in	Show ingress policies.
out	Show egress policies.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show diffserv service interface  
gigabitethernet 1/0/1 in
```

```
DiffServ Admin Mode..... Enable  
Interface..... 1/0/1  
Direction..... In
```

No policy is attached to this interface in this direction.

show diffserv service interface port-channel

Syntax Description

show diffserv service interface port-channel *channel-group* {in|out}

Parameter Description

Parameter	Description
<i>channel-group</i>	A valid port-channel in the system. (Range: 1–18)
in	Show ingress policies.
out	Show egress policies.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

Not applicable

Example

```
console#show diffserv service interface port-channel
1 in
```

```
DiffServ Admin Mode..... Enable
Interface..... pol
Direction..... In
```

No policy is attached to this interface in this direction

show diffserv service brief

Use the `show diffserv service brief` command in Privileged EXEC mode to display all interfaces in the system to which a DiffServ policy has been attached.

Syntax

```
show diffserv service brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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# show diffserv service brief
```

Interface	Direction	OperStatus	Policy Name
-----	-----	-----	-----

1/0/1	in	Down	DELL

show interfaces cos-queue

Use the `show interfaces cos-queue` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

Queue Id	Min. Bandwidth	Scheduler	Type	Queue Management Type
0	0	Weighted		Tail Drop
1	0	Weighted		Tail Drop

2	0	Weighted	Tail
Drop			
3	0	Weighted	Tail
Drop			
4	0	Weighted	Tail
Drop			
5	0	Weighted	Tail
Drop			
6	0	Weighted	Tail
Drop			

This example displays the COS configuration for the specified interface 1/0/1.

```
console#show interfaces cos-queue gigabitethernet
1/0/1
```

```
Interface..... 1/0/1
Interface Shaping Rate..... 0
```

Queue Id	Min. Bandwidth	Scheduler Type	Queue
Management	Type		
-----	-----	-----	-----

0	0	Weighted	Tail
Drop			
1	0	Weighted	Tail
Drop			
2	0	Weighted	Tail
Drop			
3	0	Weighted	Tail
Drop			

4	0	Weighted	Tail
Drop			
5	0	Weighted	Tail
Drop			
6	0	Weighted	Tail
Drop			

The following table lists the parameters in the examples and gives a description of each.

Parameter	Description
Interface	The port of the interface. If displaying the global configuration, this output line is replaced with a global configuration indication.
Intf Shaping Rate	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.
Queue Mgmt Type	The queue depth management technique used for all queues on this interface.
Queue	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.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This value is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This value is a configured value.

show interfaces random-detect

Use the `show interfaces random-detect` command in Privileged EXEC mode to display WRED policy on an interface.

Syntax

show interfaces random-detect *interface-id*

Parameter Description

Parameter	Description
interface-id	Specify an interface type. Valid interfaces include physical ports and port channels.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Use the [show interfaces cos-queue](#) command to show the global or per interface scheduler type and queue management types.

show policy-map

Use the `show policy-map` command in Privileged EXEC mode to display all configuration information for the specified policy.

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, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display policy-oriented statistics information for the specified interface.

Syntax

```
show policy-map interface {gigabithethernet unit/slot/port |
tengigabitethernet unit/slot/port / fortygigabitethernet unit/slot/port port-
channel port-channel number} {in | out}
```

Parameter Description

Parameter	Description
port-channel number	A valid 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the statistics information for port tel/0/1.

```
console#show policy-map interface tel/0/1 in
Interface..... tel/0/1
Operational Status..... Down
Policy Name..... DELL
Interface Summary:
Class Name..... PowerConnect
In Offered Packets..... 1003
In Discarded Packets..... 11
```

show service-policy

Use the `show service-policy` command in Privileged EXEC mode to display a summary of policy-oriented statistics information for all interfaces.

Syntax

```
show service-policy
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of policy-oriented statistics information.

```
console#show service-policy
```

	Oper	Policy
Intf	Stat	Name

1/0/1	Down	DELL
1/0/2	Down	DELL
1/0/3	Down	DELL
1/0/4	Down	DELL
1/0/5	Down	DELL
1/0/6	Down	DELL
1/0/7	Down	DELL
1/0/8	Down	DELL
1/0/9	Down	DELL
1/0/10	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. This process, also known as *rate shaping*, has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. To restore the default interface shaping rate value, use the **no** form of this command.

Syntax

```
traffic-shape bw kbps
```

```
no traffic-shape
```

- *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

This command has no user guidelines.

Example

The following example displays the setting of traffic-shape to a maximum bandwidth of 1024 Kbps.

```
console(config-if-1/0/1)#traffic-shape 1024 kbps
```

RADIUS Commands

Managing and determining the validity 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.

PowerConnect supports a RADIUS client in conformance with RFC 2865 and accounting functions in conformance with RFC2866. 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.

[Table 33-1](#) below indicates the RADIUS attributes supported by various PowerConnect switch service. Administrators may configure these attributes on the RADIUS server(s) when utilizing the switch RADIUS service.

Table 33-1. RADIUS Attributes Supported by PowerConnect Switch Service

Type	RADIUS Attribute Name	802.1X	User Manager	Captive Portal
1	USER-NAME	Yes	No	No
2	USER-PASSWORD	Yes	No	No

Table 33-1. RADIUS Attributes Supported by PowerConnect Switch Service

Type	RADIUS Attribute Name	802.1X	User Manager	Captive Portal
4	NAS-IP-ADDRESS	Yes	No	No
5	NAS-PORT	Yes	No	No
6	SERVICE-TYPE	No	Yes	No
11	FILTER-ID	Yes	No	No
12	FRAMED-MTU	Yes	No	No
18	REPLY-MESSAGE	Yes	Yes	No
24	STATE	Yes	Yes	No
25	CLASS	Yes	No	No
26	VENDOR-SPECIFIC	No	No	Yes
27	SESSION-TIMEOUT	Yes	No	Yes
28	IDLE-TIMEOUT	No	No	Yes
29	TERMINATION-ACTION	Yes	No	No
30	CALLED-STATION-ID	Yes	No	No
31	CALLING-STATION-ID	Yes	No	No
32	NAS-IDENTIFIER	Yes	No	No
40	ACCT-STATUS-TYPE	Set by RADIUS client for Accounting	No	No
42	ACCT-INPUT-OCTETS	Yes	No	No
43	ACCT-OUTPUT-OCTETS	Yes	No	No
44	ACCT-SESSION-ID	Set by RADIUS client for Accounting	No	No
46	ACCT-SESSION-TIME	Yes	No	No
49	ACCT-TERMINATE-CAUSE	Yes	No	No
52	ACCT-INPUT-GIGAWORDS	Yes	No	No
53	ACCT-OUTPUT-GIGAWORDS	Yes	No	No

Table 33-1. RADIUS Attributes Supported by PowerConnect Switch Service

Type	RADIUS Attribute Name	802.1X	User Manager	Captive Portal
61	NAS-PORT-TYPE	Yes	No	No
64	TUNNEL-TYPE	Yes	No	No
65	TUNNEL-MEDIUM-TYPE	Yes	No	No
79	EAP-MESSAGE	Yes	No	No
80	MESSAGE-AUTHENTICATOR	Set by RADIUS client for Accounting	No	No
81	TUNNEL-PRIVATE-GROUP-ID	Yes	No	No

The following attributes are processed in the RADIUS Access-Accept message received from a RADIUS server:

- NAS-PORT
 - ifIndex of the port to be authenticated
- REPLY-MESSAGE
 - Trigger to respond to the Access-Accept message with an EAP notification
- STATE
 - RADIUS server state. Transmitted in Access-Request and Accounting-Request messages.
- SESSION-TIMEOUT
 - Session time-out value for the session (in seconds). Used by both 802.1x and Captive Portal.
- TERMINATION-ACTION
 - Indication as to the action taken when the service is completed.
- EAP-MESSAGE
 - Contains an EAP message to be sent to the user. This is typically used for MAB clients.
- VENDOR-SPECIFIC
 - No actions configured at this time.

- **FILTER-ID**
 - Name of the filter list for this user.
- **TUNNEL-TYPE**
 - Used to indicate that a VLAN is to be assigned to the user when set to tunnel type VLAN (13).
- **TUNNEL-MEDIUM-TYPE**
 - Used to indicate the tunnel medium type. Must be set to medium type 802 (6) to enable VLAN assignment.
- **TUNNEL-PRIVATE-GROUP-ID**
 - Used to indicate the VLAN to be assigned to the user. May be a string which matches a preconfigured VLAN name or a VLAN id. If a VLAN id is given, the string must only contain decimal digits.

Commands in this Chapter

This chapter explains the following commands:

aaa accounting dot1x default start-stop	primary	radius-server timeout
accounting	priority	retransmit
acct-port	radius-server attribute 4	show aaa servers
auth-port	radius-server deadline	show accounting methods
deadline	radius-server host	show accounting methods
debug aaa accounting	radius-server key	source-ip
debug aaa accounting msgauth	radius-server retransmit	timeout
name (RADIUS server)	radius-server source-ip	usage
	–	–

aaa accounting dot1x default start-stop

The `aaa accounting network default start-stop group radius` command has been migrated to the `aaa accounting dot1x default start-stop {radius|none}` command. Use the `aaa accounting dot1x default start-stop` command in Global Config mode to create an accounting method list.

Use the `no` form of the command to delete a list. A list may be identified by the `default` keyword or a user-specified `listname`.

Use either the `aaa accounting dot1x default none` or `no aaa accounting dot1x default` command to disable dot1x accounting.

Syntax

```
aaa accounting dot1x default start-stop {radius|none }
```

```
no aaa accounting dot1x default
```

```
aaa accounting dot1x default none
```

```
aaa accounting {exec|commands} {<listname>|default} {none|start-stop|stop-only} {radius|tacacs|radius tacacs|tacacs radius}
```

```
no aaa accounting {exec|commands} {default|list}
```

Parameter Description

Parameter	Description
commands	Perform accounting on all user executed commands (TACACS only).
exec	Perform accounting on EXEC terminal sessions.
listname	The name of an Accounting Method List. The list name can consist of any printable character. Use quotes around the list name if embedded blanks are contained in the list name.
none	Disable issuing accounting notices for the specified list.

Parameter	Description
start-stop	Issue a start accounting notice at the beginning and stop accounting notice at the end of the accounted method. Accounting notices are sent when the user logs into the switch and when the user logs out of the exec mode. Accounting notifications are also sent at the beginning and at the end of the user executed command. Command execution does not wait for the accounting notification to be recorded at the AAA server.
stop-only	An accounting notice is sent when the user logs out of the exec mode. The duration of the exec session is mentioned in the accounting notice. Accounting notifications are sent at the end of each user 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.
radius	Issue accounting records to the defined RADIUS servers.
tacacs	Issue accounting records to the defined TACACS servers.

Default Configuration

IEEE 802.1x accounting is not enabled by default.

Command Mode

Global Configuration mode

User Guidelines

Accounting records, when enabled for a line mode, are sent at both the beginning and at the end (start-stop) of command execution or only at the end (stop-only) of command execution. If **none** is specified, then accounting is disabled for RADIUS. If **radius** is the specified accounting method, accounting records are forwarded to the list of RADIUS servers.

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.

A maximum of five accounting method lists can be created for each **exec** and **commands** accounting type.

The same **list-name** can be used for both **exec** and **commands** accounting types.

AAA accounting for commands with RADIUS as the accounting method is not supported. TACACS+ supports both **exec** and **commands** accounting types.

There is exactly one accounting method list for dot1x: default.

accounting

Use the **accounting** command in Line Config 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
```

Parameter Description

Parameter	Description
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. 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
```

acct-port

Use the **acct-port** command to set the port that connects to the RADIUS accounting server. 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 (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 host acct 3.2.3.2
```

```
console(Config-acct-radius)#acct-port 56
```

auth-port

Use the **auth-port** command in Radius mode to set the port number for authentication requests of the designated Radius server.

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 mode

User Guidelines

The host is not used for authentication if set to 0.

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example sets the port number 2412 for authentication requests.

```
console(config)#radius-server host 192.143.120.123
```

```
console(config-radius)#auth-port 2412
```

deadtime

Use the **deadtime** command in Radius mode to configure the minimum amount of time to wait before attempting to re-contact an unresponsive RADIUS server. 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.

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.

Command Mode

Radius mode

User Guidelines

If only one RADIUS server is configured, it is recommended to use a deadtime interval of 0.

Example

The following example specifies a deadtime interval of 60 minutes.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#deadtime 60
```

debug aaa accounting

Use the `debug aaa accounting` command in Privileged EXEC mode to enable debugging for accounting.

Use the `no` form of the command to disable accounting debugging.

Syntax

`debug aaa accounting`

`no debug aaa accounting`

Default Configuration

Debugging is disabled by default.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

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` *key-string*

- *key-string*— A string specifying the encryption key (Range: 0 - 128 characters).

Default Configuration

There is no key configured by default.

Command Mode

Radius mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies an authentication and encryption key of “*lion-king*”.

```
console(config)#radius-server host acct 3.2.3.2
console(Config-acct-radius)#key keyacct
```

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 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 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

Parameter Description

Parameter	Description
<i>servername</i>	The name for the RADIUS server (Range: 1 - 32 characters).

Default Configuration

The default RADIUS server name is Default-RADIUS-Server.

Command Mode

Radius Config mode

User Guidelines

Names may only be set for authentication servers, not for accounting servers. 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 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 ordered name server list, i.e. name1 server list would be tried before moving on to name2. Even if the priority value of servers in name2 is lower (lower value indicates high priority) the request would be sent to the name1 servers. If for name1 list, the configured servers fail to respond, the request is sent to the second configured name list.

Within the same server list, the first primary server would be tried. You can have multiple secondary servers in the same name list. From the multiple secondary servers, the one with the lowest priority value would be tried. For a different named server list, the server name would be based on lexicographic order. For e.g. if name9, name1, name6 are configured in this order, name1, then name6, then name9 would be tried.

Example

```
console(config)#radius-server host 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 the group of authentication servers which have the same server name. 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 mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config-auth-radius)#primary
```

priority

Use the **priority** command in Radius 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 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 host 192.143.120.123
console(config-radius)#priority 10
```

radius-server attribute 4

Use the **radius-server attribute 4** command in Global Configuration mode to set the network access server (NAS) IP 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 IP 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 attribute 4 value is the RADIUS server IP address.

Command Mode

Global Configuration mode

User Guidelines

This command does not change the address in the IP header for the request sent to the RADIUS server. It only changes the address sent to the RADIUS server inside the RADIUS packet.

Example

The following example sets the NAS IP address in RADIUS attribute 4 to 192.168.10.22.

```
console(config)#radius-server attribute 4  
192.168.10.22
```

radius-server deadtime

Use the **radius-server deadtime** command in Global Configuration mode to configure the minimum amount of time to wait before attempting to recontact an unresponsive RADIUS server. 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. 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.

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 host

Use the **radius-server host** command in Global Configuration mode to specify a RADIUS server host and enter RADIUS Configuration mode. To delete the specified Radius host, use the **no** form of this command.

Syntax

```
radius-server host [acct | auth] {ip-address | hostname}  
no radius-server host [acct | auth] {ip-address | hostname}
```

Parameter Description

Parameter	Description
acct auth	The type of server (accounting or authentication).
<i>ip-address</i>	The RADIUS server host IP address.
<i>hostname</i>	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, therefore it is advisable to use unique server host names.

Example

The following example specifies a Radius server host with the following characteristics:

Server host IP address — 192.168.10.1

```
console (config)#radius-server host 192.168.10.1
```

radius-server key

Use the **radius-server key** command in Global Configuration mode to set the authentication and encryption key for all Radius communications between the switch and the Radius server. To reset to the default, use the **no** form of this command.

Syntax

```
radius-server key [key-string]
```

```
no radius-server key
```

- *key-string*— Specifies the authentication and encryption key for all Radius communications between the switch and the Radius server. This key must match the encryption used on the Radius server. (Range: 1-128 characters)

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the authentication and encryption key for all Radius communications between the device and the Radius server to “dell-server.”

```
console(config)#radius-server key dell-server
```

radius-server retransmit

Use the **radius-server retransmit** command in Global Configuration mode 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 3 attempts.

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 5 attempts.

```
console(config)#radius-server retransmit 5
```

radius-server source-ip

Use the **radius-server source-ip** command in Global Configuration mode to specify the source IP address used 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 IP address of the outgoing IP interface.

Syntax

radius-server source-ip *source*

no radius-server source-ip

- *source* — Specifies the source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the source IP address used for communication with Radius servers to 10.1.1.1.

```
console(config)#radius-server source-ip 10.1.1.1
```

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 host 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 3 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 host to reply to 5 seconds.

```
console(config)#radius-server timeout 5
```

retransmit

Use the **retransmit** command in Radius 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 host 192.143.120.123
console(config-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 client.

Syntax

```
show aaa servers [accounting | authentication] [name [servername]]
```

Parameter Description

Parameter	Description
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 <i>server-name</i> name to be displayed. There are no global parameters displayed when this parameter is specified.

Default Configuration

Authentication servers are displayed by default.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Field	Description
Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Named Authentication Server Groups	The number of configured named RADIUS server groups.
Named Accounting Server Groups	The number of configured named RADIUS server groups.
Timeout	The configured timeout value, in seconds, for request retransmissions.
Retransmit	The configured value of the maximum number of times a request packet is retransmitted.
Deadtime	The length of time an unavailable RADIUS server is skipped.
RADIUS Accounting Mode	A Global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A Global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A Global parameter that specifies the IP address to be used in NAS-IP-Address attribute to be used in RADIUS requests.

Example

```
console#show aaa servers
```

IP address	Type	Port	TimeOut	Retran.	DeadTime	Source IP	Prio.	Usage
6.6.6.6	Auth	1812	Global	Global	Global	Global	0	all
5.5.5.5	Auth	1812	Global	Global	Global	Global	0	all
4.4.4.4	Auth	1812	Global	Global	Global	Global	0	all
3.3.3.3	Auth	1812	Global	Global	Global	Global	0	all
2.2.2.2	Auth	1812	Global	Global	Global	Global	0	all
1.1.1.1	Acct	1813	N/A	N/A	N/A	N/A	N/A	N/A

Global values

```
-----  
Number of Configured Authentication Servers.... 5  
Number of Configured Accounting Servers..... 1  
Number of Named Authentication Server Groups... 2  
Number of Named Accounting Server Groups..... 1  
Number of Retransmits..... 3  
Timeout Duration..... 15  
Deadtime..... 0  
Source IP..... 0.0.0.0  
RADIUS Accounting Mode..... Disable  
RADIUS Attribute 4 Mode..... Disable  
--More-- or (q)uit  
RADIUS Attribute 4 Value..... 0.0.0.0
```

```
console#show aaa servers name
```

Server Name	Host Address	Port	Secret Configured
Default-RADIUS-Server	4.4.4.4	1812	No
test	6.6.6.6	1812	No

show accounting methods

Use the `show accounting methods` command in Privileged EXEC mode to display the configured accounting method lists.

Syntax

```
show accounting methods
```

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

```
console#show accounting methods
```

```
Acct Type      Method Name      Record Type      Method Type
-----
---
Exec    dfltExecList    start-stop    TACACS
Commands  dfltCmdsList    stop-only      TACACS
Commands UserCmdAudit    start-stop      TACACS
```

```
Line      EXEC Method List      Command Method List
-----
Console  dfltExecList          dfltCmdsList
Telnet   dfltExecList          dfltCmdsList
SSH      dfltExecList          UserCmdAudit
```

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}]
```

Parameter Description

Parameter	Description
accounting authentication	The type of server (accounting or authentication).
<i>ipaddress</i>	The RADIUS server host IP address.

Parameter	Description
<i>hostname</i>	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"
<i>servername</i>	The alias used to identify the server.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed for accounting servers:

Field	Description
RADIUS Accounting Server Name	Name of the accounting server.
Server Host Address	IP address of the host.
Round Trip Time	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.
Requests	The number of RADIUS Accounting Request packets sent to this server not including the retransmissions.
Retransmissions	The number of RADIUS Accounting Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.

Field	Description
Malformed Responses	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.
Bad Authenticators	The number of RADIUS Accounting Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts on this server.
Unknown Types	The number of packets unknown type which were received from this server on accounting port.
Packets Dropped	The number of RADIUS packets received from this server on accounting port and dropped for some other reason.

The following fields are displayed for authentication servers:

Field	Description
RADIUS Server Name	Name of the authenticating server.
Server Host Address	IP address of the host.
Access Requests	The number of RADIUS Access Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access Challenge packets, including both valid and invalid packets, that were received from this server.

Field	Description
Malformed Access Responses	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.
Bad Authenticators	The number of RADIUS Access Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on authentication port and dropped for some other reason.

Example

```
console#show radius statistics accounting 192.168.37.200
```

```
RADIUS Accounting Server Name.....
Default_RADIUS_Server
Host Address.....
192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
```



```
Packets Dropped..... 0
```

```
console#show radius statistics name Default_RADIUS_Server
```

```
RADIUS Server Name.....  
Default_RADIUS_Server  
Server Host Address.....  
192.168.37.200  
Access Requests..... 0.00  
Access Retransmissions..... 0  
Access Accepts..... 0  
Access Rejects..... 0  
Access Challenges..... 0  
Malformed Access Responses..... 0  
Bad Authenticators..... 0  
Pending Requests..... 0  
Timeouts..... 0  
Unknown Types..... 0  
Packets Dropped..... 0
```

source-ip

Use the **source-ip** command in Radius 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 mode

User Guidelines

User 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-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 3 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.

```
console (config) #radius-server host 192.143.120.123
console (config-radius) #timeout 20
```

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*, *802.1x* 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) #usage login
```


Spanning Tree Commands

The Multiple Spanning Tree Protocol (MSTP) component complies with IEEE 802.1s by efficiently navigating VLAN traffic over separate interfaces for multiple instances of Spanning Tree. IEEE 802.1D, Spanning Tree and IEEE 802.1w, 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 pre-configured before mapping it to an MST instance.

Management of MSTP is compliant with the requirements of RFC5060.

The following features are supported by Power Connect 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 disables the port that is configured with this option and transitions the port into disable state. This would lead to administrative disable of the port.

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. Edge Port in an operational state is supposed to be connected to hosts that typically drop BPDUs. If an operational edge port receives a BPDU, it immediately loses its operational status. In that case, if BPDU filtering is enabled on this port then it drops the BPDUs received on this port.

STP BPDU Flooding - STP BPDU flooding feature applies to the STP disabled switch. To enable BPDU flooding on a port, STP should 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 Chapter

This chapter explains the following commands:

clear spanning-tree detected-protocols	spanning-tree auto-portfast	spanning-tree max-age	spanning-tree portfast bpdufilter default
exit (mst)	spanning-tree bpdu flooding	spanning-tree max-hops	spanning-tree portfast default
instance (mst)	spanning-tree bpdu-protection	spanning-tree mode	spanning-tree port-priority
name (mst)	spanning-tree cost	spanning-tree mst configuration	spanning-tree priority

revision (mst)	spanning-tree disable	spanning-tree mst cost	spanning-tree tanguard
show spanning-tree	spanning-tree forward-time	spanning-tree mst port-priority	spanning-tree transmit hold-count
show spanning-tree summary	spanning-tree guard	spanning-tree mst priority	–
spanning-tree	spanning-tree loopguard	spanning-tree portfast	–

clear spanning-tree detected-protocols

Use the `clear spanning-tree detected-protocols` command in Privileged EXEC mode to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

```
clear spanning-tree detected-protocols [{gigabitethernet unit/slot/port |
port-channel port-channel-number | tengigabitethernet unit/slot/port /
fortygigabitethernet unit/slot/port}]
```

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 1/0/1.

```
console#clear spanning-tree detected-protocols
gigabitethernet 1/0/1
```

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-range*

- *instance-ID* — ID of the MST instance. (Range: 1-4094)
- *vlan-range* — 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: 1-4093)

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 name.

PowerConnect 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.

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(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 tel1/1/1
console(config-if-Tel1/1/1)#switchport mode trunk
console(config-if-Tel1/1/1)#switchport trunk allowed
vlan add 2-150
console(config-if-Tel1/1/1)#spanning-tree mst 1 port-
priority 16
console(config-if-Tel1/1/1)#interface tel1/1/2
console(config-if-Tel1/1/2)#switchport mode trunk
console(config-if-Tel1/1/2)#switchport trunk allowed
vlan add 200-349
console(config-if-Tel1/1/2)#spanning-tree mst 2 port-
priority 16
console(config-if-Tel1/1/2)#exit
```

name (mst)

Use the **name** command in MST mode to define the configuration 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

This command has no user guidelines.

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

This command has no user guidelines.

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 in Privileged EXEC mode 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
```

Parameter Description

Parameter	Description
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.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following examples display spanning-tree information.

```
console#show spanning-tree
```

```
Spanning tree :Enabled - BPDU Flooding :Disabled -  
Portfast BPDU filtering :Disabled - mode :rstp
```

```
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						
-----	-----	-----	-----	-----	-----	-----

Gil/0/1	Enabled	128.1	20000	FWD	Root	No
Gil/0/2	Enabled	128.2	0	DIS	Disb	No
Gil/0/3	Enabled	128.3	0	DIS	Disb	No
Gil/0/4	Enabled	128.4	0	DIS	Disb	No

```
console#show spanning-tree gigabitethernet 1/0/1
```

```

Port Gil/0/1 Enabled
State: Forwarding                               Role:
Root
Port id: 128.1                                   Port
Cost: 20000
Port Fast: No                                    Root
Protection: No
Designated bridge Priority: 32768
Address: 0010.1882.1C53
Designated port id: 128.48
Designated path cost: 0
CST Regional Root: 80:00:00:10:18:82:1C:53      CST
Port Cost: 0
Root Guard..... FALSE
Loop Guard..... FALSE

```

```
TCN Guard..... FALSE
Auto Portfast..... TRUE
Port Up Time Since Counters Last Cleared..... 0 day
0 hr 17 min 1 sec
BPDU: sent 24, received 496
```

```
console#show spanning-tree detail
```

```
Spanning tree Enabled (BPDU flooding : Disabled)
Portfast BPDU filtering Disabled mode rstp
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
Bridge ID
                Priority          32768
                Address            001E.C9AA.AD1B
                Hello Time 2 Sec Max Age 20 sec Forward
Delay 15 sec

Number of topology changes 1 last change occurred
0d0h17m7s ago
Times: hold 6, hello 2, max age 20, forward delay 15
```

```
Port Gi1/0/1 Enabled
State: Forwarding                               Role:
Root
Port id: 128.1                                  Port
Cost: 20000
Root Protection: No
Designated bridge Priority: 32768
Address: 0010.1882.1C53
Designated port id: 128.48
Designated path cost: 0
CST Regional Root: 80:00:00:10:18:82:1C:53      CST
Port Cost: 0
BPDU: sent 24, received 500
```

```
console#show spanning-tree detail active
```

```
Spanning tree Enabled (BPDU flooding : Disabled)
Portfast BPDU filtering Disabled mode rstp
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
Bridge ID
```


Priority 32768
Address 001E.C9AA.AD1B
Hello Time 2 Sec Max Age 20 sec Forward
Delay 15 sec

Number of topology changes 1 last change occurred
0d0h17m15s ago

Times: hold 6, hello 2, max age 20, forward delay 15

Port Gi1/0/1 Enabled

State: Forwarding Role:
Root

Port id: 128.1 Port
Cost: 20000

Root Protection: No

Designated bridge Priority: 32768
Address: 0010.1882.1C53

Designated port id: 128.48
Designated path cost: 0

CST Regional Root: 80:00:00:10:18:82:1C:53 CST
Port Cost: 0

BPDU: sent 24, received 504

Port Gi1/0/5 Enabled

State: Forwarding Role:
Designated

Port id: 128.5 Port
Cost: 20000

Root Protection: No

```
Designated bridge Priority: 32768
Address: 001E.C9AA.AD1B

Designated port id: 128.5
Designated path cost: 20000

CST Regional Root: 80:00:00:1E:C9:AA:AD:1B          CST
Port Cost: 0

BPDU: sent 524, received 0
```

```
console#show spanning-tree detail blockedports

Spanning tree Enabled (BPDU flooding : Disabled)
Portfast BPDU filtering Disabled mode rstp

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

Bridge ID

                Priority          32768
                Address           001E.C9AA.AD1B
                Hello Time 2 Sec Max Age 20
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Field	Description
Spanning Tree Admin Mode	Enabled or disabled
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the mode parameter.
BPDU Protection Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
BPDU Flooding Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.

MST Instances	List of all multiple spanning tree instances configured on the switch.
---------------	--

Example

```

console#show spanning-tree summary
Spanning Tree Adminmode..... Enabled
Spanning Tree Version..... IEEE 802.1w
BPDU Guard Mode..... Disabled
BPDU Flood Mode..... Disabled
BPDU Filter Mode..... Disabled
Configuration Name..... 00-1E-C9-AA-AC-84
Configuration Revision Level..... 0
Configuration Digest Key.....
0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0

```

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. 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

Usage 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 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

`spanning-tree bpdu flooding`

`no spanning-tree bpdu flooding`

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration mode

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#spanning-tree bpdu flooding
```

spanning-tree bpdu-protection

Use the `spanning-tree bpdu-protection` command in Global Configuration mode to enable BPDU protection on a switch. Use the **no** form of this command to resume the default status of BPDU protection function.

For an access layer device, the access port is generally connected to the user terminal (such as a desktop computer) or file server directly and configured as an edge port to implement the fast transition. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree, which causes network topology flapping. In normal cases, these ports do not receive any BPDU packets. However, someone may forge BPDU to maliciously attack the switch and cause network flapping.

RSTP provides BPDU protection function against such attack. After BPDU protection function is enabled on a switch, the system disables an edge port that has received BPDU and notifies the network manager about it. The disabled port can only be enabled by the **no** version of the command.

Syntax

```
spanning-tree bpdu-protection  
no spanning-tree bpdu-protection
```

Default Configuration

BPDU protection is not enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

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 external spanning-tree path cost for a port. To return to the default port path cost, use the **no** form of this command.

Syntax

```
spanning-tree cost cost  
no spanning-tree cost
```

- *cost*— The port path cost. (Range: 0–200,000,000)

Default Configuration

The default cost is 0, which signifies that the cost is automatically calculated based on port speed.

- 10G Port path cost — 2000
- Port Channel — 20,000
- 1000 mbps (giga) — 20,000
- 100 mbps — 200,000
- 10 mbps — 2,000,000

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command configures the external cost. Since by default each switch is in its own region, the external cost is considered in determining the spanning tree of the network.

This command is also used to configure the rstp path cost.

Example

The following example configures the spanning-tree cost on 1/0/5 to 35000.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-1/0/5)#spanning-tree cost 35000
```

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 1/0/5.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-1/0/5)#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

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.

```
console(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.

```
console#config
console(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

Usage Guidelines

There are no usage 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:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

$$\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$$

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` form of this command.

Syntax

`spanning-tree mode {stp | rstp | mst}`

`no spanning-tree mode`

- `stp` — Spanning Tree Protocol (STP) is enabled.
- `rstp` — Rapid Spanning Tree Protocol (RSTP) is enabled.
- `mst` — Multiple Spanning Tree Protocol (MSTP) is enabled.

Default Configuration

Rapid Spanning Tree Protocol (RSTP) is supported.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the switch would use STP when the neighbor switch is using STP. In MSTP mode, the switch would use RSTP when the neighbor switch is using RSTP and would use STP when the neighbor switch is using STP.

Example

The following example configures the spanning-tree protocol to MSTP.

```
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 value 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

MST instance id 0 is the common internal spanning tree instance (CIST).

Example

The following example configures the MSTP instance 1 path cost for interface 1/0/9 to 4.

```
console(config)#interface gigabitethernet 1/0/9
console(config-if-1/0/9)#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
```

Parameter Description

Parameter	Description
<i>instance-id</i>	ID of the spanning-tree instance. (Range: 1-4094)
<i>priority</i>	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 16 if not an exact multiple of 16.

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
```

Parameter Description

Parameter	Description
<i>instance-id</i>	ID of the spanning-tree instance. (Range: 1-4094)
<i>priority</i>	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.

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 1/0/5.

```
console (config)#interface gigabitethernet 1/0/5
console (config-if-1/0/5)#spanning-tree portfast
```

spanning-tree portfast bpdudfilter default

The `spanning-tree portfast bpdudfilter default` command discards BPDUs received on spanning-tree ports in portfast mode. Use the “no” form of the command to disable discarding.

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

Usage Guidelines

There are no usage guidelines for this command.

Example

The following example discards BPDUs received on spanning-tree ports in portfast mode.

```
console#spanning-tree portfast bpdudfilter default
```

spanning-tree portfast default

Use the `spanning-tree portfast default` command to enable Portfast mode only on access 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

Usage Guidelines

This command only applies to 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

Use the `spanning-tree port-priority` command in Interface Configuration mode to configure port priority. To reset the default port priority, use the `no` form of this command.

Syntax

`spanning-tree port-priority priority`

`no spanning-tree port-priority`

- *priority* — The port priority. (Range: 0–240)

Default Configuration

The default port-priority for IEEE STP is 128. The default port-priority for a LAG (port-channel) is 96.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on 1/0/5 to 96.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-1/0/5)#spanning-tree port-priority
96
```

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.

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
```


TACACS+ Commands

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.

PowerConnect 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 Chapter

This chapter explains the following commands:

key	tacacs-server host
port	tacacs-server key
priority	tacacs-server timeout

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 [key-string]

- **key-string** — *To specify the key name. (Range: 1–128 characters)*

Default Configuration

If left unspecified, the key-string parameter defaults to the global value.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies an encryption and authentication key of 12.

```
console(tacacs)#key 12
```

port

Use the **port** command in TACACS Configuration mode to specify a server port number.

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 server port number 1200.

```
console(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(tacacs)#priority 10000
```

show tacacs

Use the `show tacacs` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following example displays TACACS+ server settings.

```
console#show tacacs
```

```
Global Timeout: 5
```

IP address	Port	Timeout	Priority
-----	-----	-----	-----
10.254.24.162	49	Global	0

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(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 [*key-string*]

no tacacs-server key

- *key-string* — Specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon. (Range: 0–128 printable characters except for question marks and double quotes.)

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 double quote or 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.

Example

The following example sets the authentication encryption key.

```
console(config)#tacacs-server key "I've got a secret"
console(config)#tacacs-server key @$%^&*()_+==
{}} [ < > . , / ' ; : |
```

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(tacacs)#timeout 23
```


UDLD Commands

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 will still be put into the D-Disable state 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 it is.

UDLD in Aggressive-mode

Aggressive mode differs from normal UDLD mode – it can 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 shutdown 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 Chapter

This chapter explains the following commands:

[udld enable \(Global Config\)](#)

[udld enable \(Interface Config\)](#)

[udld reset](#)

[udld port](#)

[udld message time](#)

[show udld](#)

[udld timeout interval](#)

[debug udld](#)

udld enable (Global Config)

Use the **udld enable** command in Global Config mode to enable UDLD on all physical interfaces on a switch.

Use the no form of the command to disable UDLD on all interfaces.

Syntax

udld enable

no udld enable

Default Configuration

UDLD is disabled by default.

Command Mode

Global Config mode

User Guidelines

This command globally enables UDLD. Interfaces which are not connected or enabled at the Ethernet layer at the time the command is issued will be enabled for UDLD when connected or enabled.

udld reset

Use the **udld reset** command in Privileged EXEC mode 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** in Privileged EXEC mode 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.

udld message time

Use the **udld message time** command in Global Config 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
```

Parameter Description

Parameter	Description
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 Config 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.

udld timeout interval

Use the **udld timeout interval** command in Global Config 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

udld timeout interval *timeout-interval*

no uddl timeout interval

Parameter Description

Parameter	Description
timeout-interval	UDLD timeout interval. Range is 5 to 60 seconds.

Default Configuration

The default timeout interval is 5 seconds.

Command Mode

Global Config 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.

udld enable (Interface Config)

Use the **udld enable** command in Interface (physical) Config 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 uddl enable

Default Configuration

UDLD is disabled by default on an interface.

Command Mode

Interface (physical) Config mode

User Guidelines

UDLD cannot be enabled on a port channel. Instead, enable UDLD on the physical interfaces of a port channel.

udld port

Use the **udld port** command in Interface (physical) Config 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`

Parameter Description

Parameter	Description
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 (physical) Config 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.

show uddl

Use the `show uddl` command in User EXEC or Privileged EXEC mode to display the global settings for UDLD.

Syntax

```
show uddl [interface-id | all]
```

Field Description

When no interface is specified, the following fields are shown:

Field	Description
Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.
Timeout Interval	The time period (in seconds) before making decision that link is unidirectional.

When an interface ID is specified, the following fields are shown:

Field	Description
Interface Id	The interface identifier in short form, e.g. te1/0/1.
Admin Mode	The administrative mode of UDLD configured on this interface. This is either Enabled or Disabled .
UDLD Mode	The UDLD mode configured on this interface. This is either Normal or Aggressive .

Field	Description
UDLD Status	<p>The status of the link as determined by UDLD. The options are:</p> <ul style="list-style-type: none"> • Undetermined – UDLD has not collected enough information to determine the state of the port. • Not applicable – UDLD is disabled, either globally or on the port. • Shutdown – UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • Bidirectional - UDLD has detected a bidirectional link. • Undetermined (Link Down) – The port would transition 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.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC or User EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

debug udd

Use the **debug udd** command in Privileged EXEC mode to enable the display of UDLD packets or event processing.

Use the **no** form of the command to disable debugging.

Syntax

```
debug udd {packet [receive|transmit] | events}
```

```
no debug udd {packet [receive|transmit] | events}
```

Parameter Description

Parameter	Description
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

This command has no user guidelines.

VLAN Commands

PowerConnect 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 802.1Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first 3 bits of the 802.1Q tag are used by 802.1p to establish priority for the packet.

PowerConnect 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.

PowerConnect switching supports up to 1024 VLANs for forwarding.

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.

Double VLAN Mode

An incoming frame is identified as tagged or untagged based on Tag Protocol Identifier (TPID) value it contains. The 802.1Q standard specifies a TPID value (0x8100) to recognize an incoming frame as tagged or untagged. Any valid Ethernet frame with a value 0x8100 in the 12th and 13th bytes is recognized as tagged frame. 802.1Q switches check the 12th and 13th bytes to decide the tag status of incoming frame.

The PowerConnect switching component can be configured to enable the port in double-VLAN (DVLAN) mode. In this mode switch looks for 12th, 13th, 16th, and 17th bytes for the tag status in the incoming frame. The outer tag (S-TAG) TPID is identified with the 12th and 13th bytes values. The inner tag (C-TAG) TPID is identified with 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 S-TAG value in a received frame.

PowerConnect supports configuring one outer VLAN TPID value per switch. The global default TPID is 0x88A8, which indicates a Virtual Metropolitan Area Network (VMAN).

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 PowerConnect Private VLAN feature separates a regular VLAN domain into two or more sub-domains. Each sub-domain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all sub-domains that belong to a private VLAN. The secondary VLAN ID differentiates sub-domains 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.

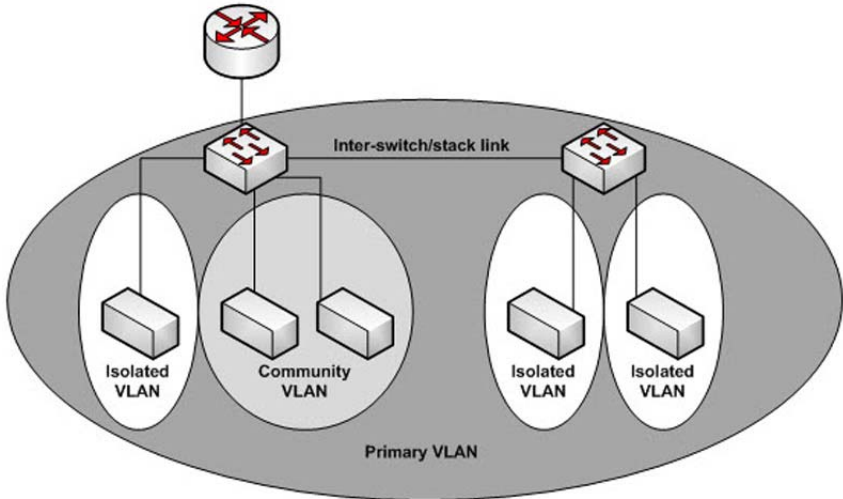
- **Isolated VLAN**
Is a secondary VLAN. It carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.
- **Community VLAN**
Is a secondary VLAN. It forwards traffic between ports which belong to the same community and to the promiscuous ports. 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 37-1](#).

Figure 37-1. Private VLANs



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 VLANs 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 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 Chapter

This chapter explains the following commands:

<code>dvlan-tunnel ethertype</code>	<code>show dvlan-tunnel interface</code>	<code>switchport general allowed vlan</code>	<code>vlan database</code>
<code>console(config-if- vlan10)#</code>	<code>show interfaces switchport</code>	<code>switchport general ingress-filtering disable</code>	<code>vlan makestatic</code>
<code>interface range vlan</code>	<code>show port protocol</code>	<code>switchport general pvid</code>	<code>vlan protocol group</code>
<code>mode dvlan-tunnel</code>	<code>show vlan</code>	<code>switchport mode</code>	<code>vlan protocol group add protocol</code>
<code>name (VLAN Configuration)</code>	<code>show vlan association mac</code>	<code>switchport trunk</code>	<code>vlan protocol group name</code>
<code>protocol group</code>	<code>show vlan association subnet</code>	<code>vlan</code>	<code>vlan protocol group remove</code>
<code>protocol vlan group</code>	<code>switchport access vlan</code>	<code>vlan (Global Config)</code>	<code>show vlan private-vlan-</code>

protocol vlan group all	switchport forbidden vlan	vlan association mac	–
show dvlan-tunnel	switchport general acceptable-frame-type tagged-only	vlan association subnet	–
Private VLAN Commands			
switchport private-vlan	private-vlan	show interfaces switchport	show vlan private-vlan
switchport mode private-vlan	–	–	–

dvlan-tunnel ethertype

Use the `dvlan-tunnel ethertype` command in Global Configuration mode to enable the configuration of the inner and outer VLAN tag ethertype.

To configure the EtherType to its default value, use the **no** form of this command.

Syntax

`dvlan-tunnel ethertype {802.1Q | vman | custom 0-65535 [primary-tpid]}`

`no dvlan-tunnel ethertype`

Parameter Description

Parameter	Description
802.1Q	Configures the EtherType as 0x8100.
vman	Configures the EtherType as 0x88A8
custom	Configures a custom EtherType for the DVLAN tunnel. The value must be 0-65535.
primary-tpid	Globally configures the tag protocol identifier on the outer VLAN tag (S-TAG). If this parameter is not given, the inner vlan (C-TAG) is configured.

Default Configuration

The default for this command is **802.1Q**. The default S-TAG TPID, when double-tagging is enabled, is 0x88A8. The default C-TAG TPID when double vlan tagging is enabled is 0x8100.

Command Mode

Global Configuration mode

User Guidelines

This command configures the TPID value on the outer VLAN (S-VLAN). The global configuration form of the command configures all physical and port-channel interfaces on which double VLAN tunneling is enabled to use the specified ethertype. Use the **mode dvlan-tunnel** command in Interface mode to enable double VLAN tagging on an interface. The interface form of the command enables/disables the use of the ethertype on the specific interface. The ethertype used in the interface form of the command must use the same ethertype as specified in the global configuration form of the command. The inner vlan tag (C-TAG) is configured using the **switchport** command in interface configuration mode.

Example

The following example displays configuring Double VLAN tunnel for vman EtherType.

```
console(config)#dvlan-tunnel ethertype vman
```

interface vlan

The **vlan routing** command is deprecated in favor of the **interface vlan** command. Use the **interface vlan** command in Global Configuration mode to enter VLAN Interface Configuration mode.

Syntax

```
interface vlan {vlan-id} [nsf-index]
```

Parameter Description

Parameter	Description
vlan-id	The ID of a valid VLAN (Range 1–4093).
nsf-index	Internal interface ID. This optional parameter is automatically generated by the system and does not need to be entered by the user. The nsf-index parameter is listed in the configuration file and the running configuration for all VLAN routing interfaces. When a nonstop forwarding failover occurs, the nsf-index enables the system to correlate checkpointed state information with the proper internal interfaces.

Default Configuration

By default, routing is enabled on VLAN 1.

Command Mode

VLAN Configuration or Global Configuration modes

User Guidelines

The **nsf-index** parameter is automatically assigned by the system for synchronizing routing information across a stack. Assigning an incorrect index via the CLI will result in an error.

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 execute a command on multiple VLANs at the same time.

Syntax

```
interface range vlan { vlan-range | all }
```

- *vlan-range* — 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: 2–4093)
- **all** — All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

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 till 228 and VLAN 889 to receive the same command.

```
console(config)#interface range vlan 221-228,889
console(config-if)#
```

mode dvlan-tunnel

Use the **mode dvlan-tunnel** command in Interface Configuration mode to enable Double VLAN Tunneling on the specified interface. To disable Double VLAN Tunneling on the specified interface, use the **no** form of this command.

Syntax

```
mode dvlan-tunnel
```

```
no mode dvlan-tunnel
```

Default Configuration

By default, Double VLAN Tunneling is *disabled*.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

Use the global configuration command `dvlan-tunnel ethertype` to configure the inner and outer TPIDs.

Example

The following example displays how to enable Double VLAN Tunneling at gigabit ethernet port 1/0/1.

```
console(config-if-1/0/1)#mode dvlan-tunnel
```

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

Parameter Description

Parameter	Description
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"
```

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 groupid vlanid
```

```
no protocol group groupid vlanid
```

- *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.
- *vlanid*— 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#vlan database
console(config-vlan)#protocol group 3 100
```

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 groupid
no protocol vlan group groupid
```

- *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.

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 a physical port interface to the group ID of "2."

```
console(config-if-1/0/1)#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 groupid
```

```
no protocol vlan group all groupid
```


- *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.

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 dvlan-tunnel

Use the **show dvlan-tunnel** command in Privileged EXEC mode to display all interfaces enabled for Double VLAN Tunneling.

Syntax

```
show dvlan-tunnel
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display all interfaces for Double VLAN Tunneling.

```
console#show dvlan-tunnel
Interfaces Enabled for DVLAN Tunneling..... 1/0/1
```

show dvlan-tunnel interface

Use the `show dvlan-tunnel interface` command in Privileged EXEC mode to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Syntax

```
show dvlan-tunnel interface {gigabitethernet unit/slot/port |
tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port | all}
```

- `all` — Displays information for all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays detailed information for port 1/0/1.

```
console#show dvlan-tunnel interface 1/0/1
```

```
Interface  Mode      EtherType
-----  -
1/0/1      Enable  vMAN
```

The following table describes the significant fields shown in the example.

Field	Description
Mode	This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is <i>disabled</i> .
Interface	Interface Number.
EtherType	This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. The three different EtherType tags are: (1) 802.1Q, which represents the commonly used value of 0x8100. (2) vMAN, which represents the commonly used value of 0x88A8. (3) If EtherType is not one of these two values, it is a custom tunnel value, representing any value in the range of 0 to 65535.

show interfaces switchport

Use the `show interfaces switchport` command in Privileged EXEC mode to display switchport configuration, including the private VLAN mappings.

Syntax

```
show interfaces switchport {{gigabitethernet unit/slot/port | port-channel
port-channel-number | tengigabitethernet unit/slot/port |
fortygigabitethernet unit/slot/port}}
```

Parameter Description

The command displays the following information.

Parameter	Description
private-vlan host-association	Displays VLAN association for the private-VLAN host ports.
private-vlan mapping	Displays VLAN mapping for the private-VLAN promiscuous ports.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Interface Config mode and all Config sub-modes

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.

Examples

The following example displays switchport configuration individually for gi1/0/1.

```
console#show interface switchport gigabitethernet 1/0/1
```

```
Port 1/0/1:
```

```
VLAN Membership mode: General
```

```
Operating parameters:
```

```
PVID: 1 (default)
```

```
Ingress Filtering: Enabled
```

```
Acceptable Frame Type: All
```

```
GVRP status: Enabled
```

```
Protected: Enabled
```

```
Port 1/0/1 is member in:
```

VLAN	Name	Egress rule	Type
----	-----	-----	-----
1	default	untagged	Default

8	VLAN008	tagged	Dynamic
11	VLAN0011	tagged	Static
19	IPv6 VLAN	untagged	Static
72	VLAN0072	untagged	Static

Static configuration:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

Port 1/0/1 is statically configured to:

VLAN	Name	Egress rule
----	-----	-----
11	VLAN0011	tagged
19	IPv6 VLAN	untagged
72	VLAN0072	untagged

Forbidden VLANs:

VLAN	Name
----	-----
73	Out

The following example displays switchport configuration individually for 1/0/2.

```
console#show interface switchport gigabitethernet
1/0/2
```

Port 1/0/2:

VLAN Membership mode: General

Operating parameters:

PVID: 4095 (discard vlan)

Ingress Filtering: Enabled

Acceptable Frame Type: All

Port 1/0/1 is member in:

VLAN	Name	Egress rule	Type
-----	-----	-----	-----
91	IP Telephony	tagged	Static

Static configuration:

PVID: 8

Ingress Filtering: Disabled

Acceptable Frame Type: All

Port 1/0/2 is statically configured to:

VLAN	Name	Egress rule
-----	-----	-----
8	VLAN0072	untagged
91	IP Telephony	tagged

Forbidden VLANS:

VLAN	Name
-----	-----
73	Out

The following example displays switchport configuration individually for 2/0/19.

```
console#show interfaces switchport gigabitethernet 2/0/19
```

Port 2/0/19:

Operating parameters:

PVID: 2922

Ingress Filtering: Enabled

Acceptable Frame Type: Untagged

GVRP status: Disabled

Port 2/0/19 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	-----
2921	Primary A	untagged	Static
2922	Community A1	untagged	Static

Static configuration:

PVID: 2922

Ingress Filtering: Enabled

Acceptable Frame Type: Untagged

GVRP status: Disabled

Port 2/0/19 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	-----
2921	Primary A	untagged	Static
2922	Community A1	untagged	Static

show port protocol

Use the **show port protocol** command in Privileged EXEC mode to display the Protocol-Based VLAN information for either the entire system or for the indicated group.

Syntax

```
show port protocol {groupid | all}
```

- *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.
- `all` — Enter `all` to show all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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
```

Group		Group			
Group Name	ID	Protocol(s)	VLAN	Interface(s)	
-	-	-	-	-	-
test	1	IP	1	1/0/1	

show vlan

Use the `show vlan` command in Privileged EXEC mode to display detailed information, including interface information and dynamic VLAN type, for a specific VLAN. The ID is a valid VLAN identification number.

Syntax

```
show vlan [id vlanid /name vlan-name]
```


Parameter Description

Parameter	Description
vlanid	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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays information for VLAN id 1, 2 and 3.

```
console#show vlan id 1
```

VLAN	Name	Ports	Type
1	default	Po1-48, Gi1/0/1-10	Default

```
console#show vlan id 2
```

VLAN	Name	Ports	Type
2	VLAN0002 (DOT1X)	Gi1/0/11-20	Dynamic

```
console#show vlan id 3
```

VLAN	Name	Ports	Type
3	VLAN0003 (GVRP)	Gi1/0/21-24	Dynamic

show vlan association mac

Use the `show vlan association mac` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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

console#

show vlan association subnet

Use the **show vlan association subnet** command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

The command has no user guidelines.

Example

The following example shows the case if no IP Subnet to VLAN association exists.

```
console#show vlan association subnet
IP Address          IP Mask            VLAN ID
-----
```

The IP Subnet to VLAN association does not exist.

switchport access vlan

Use the `switchport access vlan` command in Interface Configuration mode to configure the VLAN ID when the interface is in access mode. To reconfigure the default, use the `no` form of this command.

Syntax

```
switchport access vlan vlan-id
```

```
no switchport access vlan
```

- *vlan-id*— A valid VLAN ID of the VLAN to which the port is configured.

Default Configuration

The default value for the *vlan-id* parameter is 1.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of interface 1/0/8 to become an access member of VLAN ID 23.

```
console(config)#interface gigabitethernet 1/0/8
```

```
console(config-if-1/0/8)#switchport access vlan 23
```

switchport forbidden vlan

Use the `switchport forbidden vlan` command in Interface Configuration mode to forbid adding specific VLANs to a port. To revert to allowing the addition of specific VLANs to the port, use the `remove` parameter of this command.

Syntax

`switchport 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 (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command has no user guidelines.

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-1/0/8)#switchport forbidden vlan
add 234-256
```

switchport 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 (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 1/0/8 to discard untagged frames at ingress.

```
console(config)#interface gigabitethernet 1/0/8  
console(config-if-1/0/8)#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 (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

You can use this command to change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

Example

The following example shows how to add VLANs 1, 2, 5, and 8 to the allowed list.

```
console(config-if-1/0/8)#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

This command has no user guidelines.

Example

The following example shows how to enable port ingress filtering on 1/0/8.

```
console(config)#interface gigabitethernet 1/0/8  
console(config-if-1/0/8)#switchport general ingress-  
filtering disable
```

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

This command has no user guidelines.

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-1/0/8)#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
```

Parameter Description

Parameter	Description
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. An access port transmits only untagged packets.

Parameter	Description
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 PVID. A trunk only transmits tagged packets.
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 for this command 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 1/0/5 to access mode.

```
console(config)#interface gigabitethernet 1/0/5
console(config-if-1/0/5)#switchport mode access
```

switchport trunk

Use the **switchport trunk** command in Interface Configuration mode to add VLANs to or remove VLANs from a trunk port, or to set the PVID for an interface in Trunk Mode.

Syntax

```
switchport trunk {allowed vlan vlan-list | native vlan vlan-id}
```

Parameter Description

Parameter	Description
vlan-list	<p>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:</p> <p>The vlan-list format is all [add remove except] vlan-atom [, vlan-atom...] where:</p> <p>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.</p> <p>add adds the defined list of VLANs to those currently set instead of replacing the list.</p> <p>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.</p> <p>except lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)</p> <p>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.</p>
valid-id	A valid VLAN id from 1-4093.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (gigabitethernet, port-channel, tengigabitethernet, fortygigabitethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
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
```

vlan

Use the `vlan` command in VLAN Database mode to configure a VLAN. To delete a VLAN, use the `no` form of this command.

Syntax

```
vlan vlan-range
```

```
no vlan vlan-range
```

- *vlan-range* — A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2–4093)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

Deleting the VLAN for an access port will cause that port to become unusable until it is assigned a VLAN that exists.

Example

The following example shows how to create (add) VLAN of IDs 22, 23, and 56.

```
console(config-vlan)#vlan 22,23,56
```

```
console(config-vlan)#
```

vlan (Global Config)

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-id | vlan-range }  
no vlan { vlan-id | vlan-range }
```

Parameter Description

Parameter	Description
<i>vlan-id</i>	A valid VLAN ID. (Range: 2–4093)
<i>vlan-range</i>	A list of valid VLAN IDs. List separate, non-consecutive VLAN IDs separated by commas (without spaces). Use a hyphen to designate a range of IDs. (Range: 2–4093)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration (Config)

User Guidelines

This command has no user guidelines.

Example

The following example shows how to create (add) VLAN of IDs 22, 23, and 56.

```
console(config)#vlan 22,23,56  
console(config-vlan)#
```

vlan association mac

Use the `vlan association mac` command in VLAN Config mode to associate a MAC address to a VLAN. The maximum number of MAC-based VLANs is 256. Only packets with a matching source IP 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`)

Default Configuration

No assigned MAC address.

Command Mode

VLAN Config mode

User Guidelines

This command has no user guidelines.

Example

The following example associates MAC address with VLAN ID 1.

```
console(config)# interface vlan 1
console(config-vlan-1)#vlan association mac
0001.0001.0001
```

vlan association subnet

Use the `vlan association subnet` command in VLAN Config 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 Config 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)#interface vlan 1
console(config-vlan-1)#vlan association subnet
192.168.0.0 255.255.255.0
```

vlan database

Use the **vlan database** command in Global Configuration mode to enter the VLAN database configuration mode.

Syntax

vlan database

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 VLAN database mode.

```
console (config) #vlan database
console (config-vlan) #
```

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

VLAN Database 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.

In previous implementations, when multiple VLAN protocol groups were created, and then one of the groups was deleted and the configuration was saved, this command resulted in an incorrect application of the group IDs upon reload. So, the existing command **vlan protocol group *groupname*** is updated to **vlan protocol group *groupid*** so that **groupid** is used for both configuration and script generation.



NOTE: If an attempt is made to migrate to the latest implementation with any of the group names deleted prior to saving configuration on the pre 3.1.4.x code (applicable only for platforms PC8024/PC8024F), the problem on the latest code will remain.

Syntax

```
vlan protocol group groupid
```

```
no vlan protocol group groupid
```

- *groupid*— 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 *groupid* *ethertype* *value*

no vlan protocol group add protocol *groupid* *ethertype* *value*

- *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.
- *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 groupid groupName
```

```
no vlan protocol group name groupid
```

- *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 groupid`

- *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.

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 private-vlan

Use the `switchport private-vlan` command in Interface Config 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

```
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}
```

Parameter Description

Parameter	Description
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.

switchport mode private-vlan

Use the `switchport mode private-vlan` command in Interface Config 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
```

Parameter Description

Parameter	Description
host-association	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.

private-vlan

Use the **private-vlan** command in VLAN Config 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]

Parameter Description

The command displays the following information:

Parameter	Description
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 Config 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
console(config)# vlan 20
console(config-vlan)# private-vlan association 1001-1003
console(config-vlan)# end
```

show vlan private-vlan

Use the **show vlan private-vlan** command in Privileged EXEC mode 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]
```


Parameter Description

The command displays the following information.

Parameter	Description
Primary	Primary VLAN ID.
Secondary	Secondary VLAN ID.
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.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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.

Voice VLAN Commands

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 the LLDP-MED mechanism. The voice data coming from the VoIP phone is tagged with the exchanged VLAN ID; thus, regular data arriving on the switch is given the default PVID of the port, and the voice traffic is received on a predefined VLAN. The two types of traffic are therefore segregated so that better service can be provided to the voice traffic.

When a dot1p priority is associated with the voice VLAN port instead of VLAN ID, then the priority information is passed onto the VoIP phone using the LLDP-MED mechanism. Thus, the voice data coming from the VoIP phone is tagged with VLAN 0 and with the exchanged priority. Regular data arriving on the switch is given the default priority of the port (default 0), and the voice traffic is received with higher priority, thus segregating both the traffic to provide better service to the voice traffic.

The switch can be configured to override the data traffic CoS. This feature enables overriding the 802.1P priority of the data traffic packets arriving at the port enabled for voice VLAN. Thus, a rogue client that is also connected to the voice VLAN port does not deteriorate the voice traffic. Voice VLAN is recommended for enterprise-wide deployment of voice services on the IP network.

Commands in this Chapter

This chapter explains the following commands:

voice vlan	voice vlan data priority
voice vlan (Interface)	show voice vlan

voice vlan

This command is used to enable the voice vlan capability on the switch.

Syntax

voice vlan

no voice vlan

Parameter Ranges

Not applicable

Command Mode

Global Configuration

Usage Guidelines

Not applicable

Default Value

This feature is disabled by default.

Example

```
console(config)#voice vlan
```

```
console(config)#no voice vlan
```

voice vlan (Interface)

This command is used to enable the voice vlan capability on the interface.

Syntax

`voice vlan { vlanid | dot1p priority | none | untagged | data priority {trust | untrust} | auth { enable | disable } | dscp dscp }`

`no voice vlan`

Parameter Description

Parameter	Description
<code>auth</code>	Enables/disables authentication on the voice vlan port.
<code>data</code>	Observe the priority on received voice vlan traffic (trusted mode).
<code>dot1p</code>	Configure Voice VLAN 802.1p priority tagging for voice traffic.
<code>dscp</code>	Configure DSCP value for voice traffic on the voice vlan port. (Range: 0–64).
<code>none</code>	Allow the IP phone to use its own configuration to send untagged voice traffic.
<code>priority</code>	The Dot1p priority for the voice VLAN on the port.
<code>trust</code>	Trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
<code>untagged</code>	Configure the phone to send untagged voice traffic.
<code>untrust</code>	Do not trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
<code>vlanid</code>	The voice VLAN ID.

Default Configuration

The default DSCP value is 46.

Command Mode

Interface Configuration (Ethernet) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-Gi1/0/1)#voice vlan 1
console(config-if-Gi1/0/1)#voice vlan dot1p 1
console(config-if-Gi1/0/1)#voice vlan none
console(config-if-Gi1/0/1)#voice vlan untagged
```

voice vlan data priority

This command is to either trust or not trust (untrust) the data traffic arriving on the voice VLAN port.

Syntax

`voice vlan data priority {trust | untrust}`

- **trust**—Trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
- **untrust**—Do not trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.

Command Mode

Interface Configuration

Default Value

trust

Example

```
console(config-if-1/0/1)#voice vlan data priority untrust
console(config-if-1/0/1)#voice vlan data priority trust
```

show voice vlan

```
show voice vlan [interface {gigabitethernet unit/slot/port |
tengigabitethernet unit/slot/port | fortygigabitethernet unit/slot/port | all}]
```

Syntax

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:

When the interface parameter is specified:	
Voice VLAN Mode	The admin mode of the voice VLAN on the interface.
Voice VLAN ID	The voice VLAN ID.
Voice VLAN Priority	The Dot1p priority for the voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the voice VLAN traffic.
Voice VLAN COS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of voice VLAN on the port.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

Example

```
(console) #show voice vlan interface 1/0/1
```

```
Interface.....1/0/1
Voice VLAN Interface Mode.....Enabled
Voice VLAN ID.....1
Voice VLAN COS Override.....False
Voice VLAN Port Status.....Disabled
```


802.1x Commands

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 PowerConnect supports an 802.1x Authenticator service with a local authentication server or authentication using remote RADIUS or TACACS servers.

Supported security methods for communication with remote servers include MD5, PEAP, EAP-TTL, EAP-TTLS, and EAP-TLS.

Local 802.1X Authentication Server

The PowerConnect switch supports a dedicated database for local authentication of users for network access through the Dot1x feature. This functionality is distinct from management access for the switch. This feature supports creating users for Dot1x (port) access only.

The Internal Authentication Server feature provides support for the creation of users for Dot1x access only, i.e. without management access. This feature maintains a separate database (henceforth called as Dot1x user database) of users allowed for Dot1x access.

A new authentication method **internal** is added to the list of methods supported by authentication list creation in order to support the IDAS user database lookup. The **internal** 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 Dot1x authentication mode and selects the authentication method as internal, then the user credentials received from the Dot1x supplicant is validated against the IDAS by Dot1x component. The Dot1x application accesses the Dot1x 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 Dot1x state machine to send a challenge to the supplicant. Otherwise a failure is returned to the Dot1x 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 dot1x users and their attributes. The Dot1x maintained user database can be exported (uploaded) or imported (downloaded) to/from a central location using a TFTP server.

MAC Authentication Bypass

Today, 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 and MAB cannot be supported independent of the Dot1x 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 pre-populated in the authentication server. MAB only works when the port control mode of the port is MAC-based.

Port access by MAB clients is allowed if the Dot1x user database has corresponding entries added for the MAB clients with user name and password attributes set to the MAC address of MAB clients.

Guest VLAN

The Guest VLAN feature allows a PowerConnect switch to provide a distinguished service to unauthenticated users (not rogue users who fail authentication). This feature provides a mechanism to allow visitors and contractors to have network access to reach external network with no ability to surf 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. Therefore, 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 access to the client.

802.1x Monitor Mode

Monitor mode is a special mode that can be enabled in conjunction with Dot1x 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 Dot1x 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 Dot1x 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 VLAN, regardless of the RADIUS assignment.

RADIUS-based Dynamic VLAN Assignment

If VLAN assignment is enabled in the RADIUS server then as part of the response message, the RADIUS server sends the VLAN ID which the client is requested to use in the 802.1x tunnel attributes. If dynamic VLAN creation is enabled on the switch and the RADIUS assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and be assigned to the appropriate VLAN. This gives flexibility for clients to move around the network with out requiring the operator to perform additional provisioning for each network interface.

Commands in this Chapter

This chapter explains the following commands:

<code>dot1x dynamic-vlan enable</code>	<code>dot1x system-auth-control monitor</code>	<code>show dot1x clients</code>
<code>dot1x initialize</code>	<code>dot1x timeout guest-vlan-period</code>	<code>show dot1x interface</code>
<code>dot1x mac-auth-bypass</code>	<code>dot1x timeout quiet-period</code>	<code>show dot1x interface statistics</code>
<code>dot1x max-req</code>	<code>dot1x timeout re-authperiod</code>	<code>show dot1x users</code>
<code>dot1x max-users</code>	<code>dot1x timeout server-timeout</code>	<code>clear dot1x authentication-history</code>
<code>dot1x port-control</code>	<code>dot1x timeout supp-timeout</code>	<code>dot1x guest-vlan</code>
<code>dot1x re-authenticate</code>	<code>dot1x timeout tx-period</code>	<code>dot1x unauth-vlan</code>
<code>dot1x reauthentication</code>	<code>show dot1x</code>	<code>show dot1x advanced</code>

[dot1x system-auth-control](#) [show dot1x authentication-history](#) –

802.1x Advanced Features

dot1x guest-vlan	dot1x unauth-vlan	show dot1x advanced
----------------------------------	-----------------------------------	-------------------------------------

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`

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is Disabled.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

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]
```

Syntax Description

Parameter	Description
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.

dot1x mac-auth-bypass

Use the `dot1x mac-auth-bypass` command to enable MAB on an interface. Use the `no` form of this command to disable MAB on an interface.

Syntax

```
dot1x mac-auth-bypass  
no dot1x mac-auth-bypass
```

Default Configuration

MAC Authentication Bypass is disabled by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Authentication of a user via `mac-auth-bypass` will not occur until the "`dot1x time-out guest-vlan-period`" timer expires.

Example

The following example sets MAC Authentication Bypass on interface 1/2:

```
console (config-if-1/0/2) #dot1x mac-auth-bypass
```

dot1x max-req

Use the `dot1x max-req` command in Interface Configuration mode to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client 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.

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-1/0/16)# 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: 1–16)

Default Configuration

The default number of clients supported on a port with MAC-based 802.1X authentication is 8.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following command limits the number of devices that can authenticate on port 1/0/2 to 3.

```
console(config-if-1/0/2)#dot1x max-users 3
```


dot1x port-control

Use the **dot1x port-control** command in Interface Configuration mode to enable the IEEE 802.1X operation on the port.

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.
- **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.
- **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.
- **mac-based** — Enables 802.1x authentication on the interface and allows multiple hosts to authenticate on a single port. The hosts are distinguished by their MAC addresses.

Default Configuration

The default configuration is **auto**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended that you disable the 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-1/0/2)# dot1x port-control mac-
based
```

dot1x re-authenticate

Use the **dot1x re-authenticate** command in Privileged EXEC mode to enable manually initiating 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

This command has no user guidelines.

Example

The following command manually initiates a re-authentication 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 re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables periodic re-authentication of the client.

```
console(config)# interface gigabitethernet 1/0/16  
console(config-if-1/0/16)# 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

This command has no user guidelines.

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
```

Parameter Description

This command has no arguments or keywords.

Default Configuration

Dot1x monitor mode is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables 802.1x globally.

```
console(config)# dot1x system-auth-control monitor
```

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 dot1x 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 dot1x unaware client.

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 `while` timer so that at least three EAP Requests are sent, before assuming that the client is a dot1x unaware client.

Example

The following example sets the `dot1x timeout guest-vlan-period` to 100 seconds.

```
console(config)# dot1x timeout guest-vlan-period 100
```

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-1/0/16)# 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 re-authentication 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

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

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-1/0/16)# 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-1/0/1)# dot1x timeout server-  
timeout 3600
```

dot1x timeout supp-timeout

Use the `dot1x timeout supp-timeout` command in Interface Configuration mode to set the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request 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— 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 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 example sets the time for the retransmission of an EAP-request frame to the client to 3600 seconds.

```
console(config-if-1/0/1)# dot1x timeout supp-timeout
3600
```

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-1/0/16)# dot1x timeout tx-period
3600
```

show dot1x

Use the `show dot1x` command in Privileged EXEC mode 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]]
```

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

If you do not use the optional parameters, the command displays the global dot1x mode and the VLAN Assignment mode.

Field	Description
<i>Administrative Mode</i>	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS assigned VLAN is allowed (enabled) or not (disabled).
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

Example

```
console#show dot1x
Administrative Mode.....Enabled
VLAN Assignment Mode.....Disabled
Monitor Mode.....Disabled
```

show dot1x authentication-history

Use the `show dot1x authentication-history` command in Privileged EXEC mode 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]
```

Parameter Description

The following table explains the output parameters.

Parameter	Description
Time Stamp	Exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
MAC-Address	Supplicant/Client MAC Address
VLAN assigned	VLAN assigned to the client/port on authentication.
VLAN assigned Reason	Type of VLAN ID assigned i.e Guest VLAN, Unauth, Default, Radius Assigned or Monitor Mode VLAN ID.
Auth Status	Authentication Status
Reason	Actual reason behind the successful or failure authentication.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show dot1x authentication-history all detail
```

```
Time Stamp..... Mar 22 2010  
01:16:31
```

```
Interface..... Gi1/0/2
```

```
MAC-Address.....  
00:01:02:03:04:05
```

```
VLAN Assigned..... 111
```

```
VLAN Assigned Reason..... Guest VLAN
```

```
Auth Status..... Authorized
```

```
Reason..... Dot1x  
Authentication
```

```
due to Guest
```

```
VLAN
```

```
Timer Expiry.
```

```
.....
```

```
.....
```

```
console#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
```

```
console#show dot1x authentication-history gil/0/1
```

```
Time Stamp          Interface MAC-Address  
VLANID Auth Status
```

```
-----  
-----
```

```
Mar 22 2010 01:16:31 gil/0/1  00:01:02:03:04:05 111  
Authorized
```

```
Mar 22 2010 01:18:22 gil/0/1  00:00:00:03:04:05 0  
Unauthorized
```

```
console#show dot1x authentication-history gil/0/1  
failed-auth-only
```

```
Time Stamp          Interface MAC-Address  
VLANID Auth Status
```

```
-----  
-----
```

```
Mar 22 2010 01:18:22 gil/0/2  00:00:00:03:04:05 0  
Unauthorized
```

show dot1x clients

Use the `show dot1x clients` command in Privileged EXEC mode 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}
```

Parameter Description

Parameter	Description
<i>interface-id</i>	Any valid interface. See Interface Naming Conventions for interface representation.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed by this command.

Field	Description
<i>Clients Authenticated using Monitor Mode</i>	Indicates the number of Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.

The following table describes the significant fields shown in the display.

Field	Description
Interface	The port number.
Username	The username representing the identity of the Supplicant. This field shows the username when the port control is auto or mac-based . 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.
Supp MAC Address	The MAC-address of the supplicant
Session Time	The amount of time, in seconds, since the client was authenticated on the port.

Field	Description
Filter ID	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 and client.
VLAN Assigned	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.

Example

The following example displays information about the 802.1x clients.

```

console#show dot1x clients all

Clients Authenticated using Monitor Mode..... 1
Clients Authenticated using Dot1x..... 1

Logical Interface..... 16
Interface.....
gi1/0/2

User Name.....
000102030405

Supp MAC Address.....
00:01:02:03:04:05

Session Time..... 518
Filter Id.....
VLAN Id..... 1
VLAN Assigned.....
Default

Session Timeout..... 0
Session Termination Action.....
Default

```



```

Logical Interface..... 96
Interface.....
gi1/0/7
User Name..... brcm
Supp MAC Address.....
00:08:A1:7E:45:1A
Session Time..... 67
VLAN Id..... 1
VLAN Assigned.....
Monitor Mode
Session Timeout..... 0
Session Termination Action.....
Default

```

show dot1x interface

This command shows the status of MAC Authentication Bypass. This feature is an extension of Dot1x Option 81 feature added in Power Connect Release 2.1. to accept a VLAN name as an alternative to a number when RADIUS indicates the Tunnel-Private-Group-ID for a supplicant.

Syntax

```
show dot1x interface {gigabitethernet unit/slot/port | tengigabitethernet
unit/slot/port | fortygigabitethernet unit/slot/port}
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show dot1x interface gigabitethernet 1/0/10
```

```
Administrative Mode..... Disabled
Dynamic VLAN Creation Mode..... Disabled
Monitor Mode..... Disabled
```

Port	Admin	Oper	Reauth
Reauth	Mode	Mode	Control
Period			
-----	-----	-----	-----

Gi1/0/10	auto	N/A	FALSE
3600			

```
Quiet Period..... 60
Transmit Period..... 30
Maximum Requests..... 2
Max Users..... 16
VLAN Assigned.....
Supplicant Timeout..... 30
Guest-vlan Timeout..... 30
Server Timeout (secs)..... 30
```

```

MAB mode (configured).....
Disabled

MAB mode (operational).....
Disabled

Authenticator PAE State.....
Initialize

Backend Authentication State.....
Initialize

```

show dot1x interface statistics

Use the `show dot1x interfacestatistics` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x statistics for the specified interface.

```
console#show dot1x interface gigabitethernet 1/0/2
statistics
```

```
Port..... gi1/0/2
```

```

EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0
EAPOL Logoff Frames Received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source.....
0000.0000.0000
EAP Response/Id Frames Received..... 0
EAP Response Frames Received..... 0
EAP Request/Id Frames Transmitted..... 0
EAP Request Frames Transmitted..... 0
Invalid EAPOL Frames Received..... 0
EAPOL Length Error Frames Received..... 0
The following table describes the significant fields shown in the display.

```

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.

Field	Description
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

show dot1x users

Use the **show dot1x users** command in Privileged EXEC mode to display 802.1x authenticated users for the switch.

Syntax

show dot1x users [*username username*]

- *username* — Supplicant username (Range: 1–160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x users.

```
console#show dot1x users
Port      Username
-----
1/0/1     Bob
1/0/2     John
Switch# show dot1x users username Bob
Port      Username
-----
1/0/1     Bob
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The username representing the identity of the Supplicant.
Port	The port that the user is using.

clear dot1x authentication-history

Use the `clear dot1x authentication-history` command in Privileged EXEC mode to clear the authentication history table captured during successful and unsuccessful authentication.

Syntax

```
show dot1x authentication-history [interface-id]
```

Parameter Description

Parameter	Description
<code>interface-id</code>	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

```
console#clear dot1x authentication-history
```

Purge all entries from the log.

```
console#clear dot1x authentication-history gil/0/1
```

Purge all entries for the specified interface from the log.

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 already have been defined. 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: 0-4093).

Default Configuration

The guest VLAN is disabled on the interface by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Configure the guest VLAN before using this command.

Example

The following example sets the guest VLAN on port 1/0/2 to VLAN 10.

```
console(config-if-1/0/2)#dot1x guest-vlan 10
```

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: 0-4093).

Default Configuration

The unauthenticated VLAN is disabled on the interface by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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-1/0/2)#dot1x unauth-vlan 20
```

show dot1x advanced

Use the **show dot1x advanced** command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 VLAN	Unauthenticated Vlan
-----	-----	-----

1/0/1	Disabled	Disabled
1/0/2	10	20
1/0/3	Disabled	Disabled
1/0/4	Disabled	Disabled
1/0/5	Disabled	Disabled
1/0/6	Disabled	Disabled

```
console#show dot1x advanced gigabitethernet 1/0/2
```

Port	Guest VLAN	Unauthenticated Vlan
-----	-----	-----
1/0/2	10	20

Data Center Technology Commands

NOTE: Fiber Channel over Ethernet (FCoE) commands are only supported on the PC8024 and PC8024F switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.

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.

This section of the document contains the following FCoE commands:

[Data Center Bridging Commands](#)

[FIP Snooping Commands](#)

[Priority Flow Control Commands](#)

Data Center Bridging Commands

NOTE: Fiber Channel over Ethernet (FCoE) commands are only supported on the PC8024 and PC8024F 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 PowerConnect 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

Overview

In a typical switch or router, each physical 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 PowerConnect 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 PowerConnect 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 PowerConnect switches in release 4.2.

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 PowerConnect 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 PowerConnect 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. 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

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. Specifically, the willing parameter is disabled on auto-downstream. 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 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. 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.

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, all auto-upstream ports other than the configuration source are marked as willing disabled.

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 Chapter

This chapter explains the following commands:

Data Center Bridging Capability Exchange Commands

<code>datacenter-bridging</code>	<code>lldp dcbx port-role</code>
<code>lldp dcbx version</code>	<code>show lldp tlv-select</code>
<code>lldp tlv-select dcbxp</code>	<code>show lldp dcbx</code>

Enhanced Transmission Selection Commands

<code>classofservice traffic-class-group</code>	<code>traffic-class-group weight</code>
<code>traffic-class-group max-bandwidth</code>	<code>show classofservice traffic-class-group</code>
<code>traffic-class-group min-bandwidth</code>	<code>show interfaces traffic-class-group</code>
<code>traffic-class-group strict</code>	—

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


This command has no user guidelines.

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
```

Parameter Description

Parameter	Description
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

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.

Example

The following example configures the switch to use CEE DCBX.

```
s1(config)#lldp dcbx version cee
```

lldp tlv-select dcbxp

Use the `lldp tlv-select dcbxp` command in Global Configuration or Interface Configuration mode to enable the LLDP to send DCBX TLVs if LLDP is enabled to transmit on the given interface. If no parameter is given, all DCBX TLVs are enabled for transmission. The default is all DCBX TLVs are enabled for transmission. If executed in Interface mode, the interface configuration overrides the global configuration for that interface. Entering the command with no parameters enables transmission of all TLVs.

Use the `no` form of the command to return the configuration to the default settings.

Syntax

`lldp tlv-select dcbxp [ets-config|ets-recommend|pfc|application-priority|congestion-notification]`

`no lldp tlv-select dcbxp [ets-config|ets-recommend|pfc|application-priority|congestion-notification]`

Parameter Description

Parameter	Description
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.

Default Configuration

The default value is to transmit all TLVs as enabled by the auto-configuration port role. In manual mode, the default is to transmit all TLVs.

Command Mode

Global Config, Interface Config

User Guidelines

Interface configuration overrides the global configuration on the designated interface. The PC8024 proxies ETS TLVs received from the configuration source to the other auto-configured ports while not acting upon them. The PC81xx both processes and proxies ETS TLVs received from the configuration source as well as generates ETS TLVs on manually configured ports.

Example

The following example configures the port to transmit all TLVs.

```
console(interface-config-te1/0/1)#no lldp tlv-select dcbxp
```


Ildp dcbx port-role

Use the `ildp 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

```
ildp dcbx port-role {auto-up | auto-down | manual | configuration-source}
```

Parameter Description

Parameter	Description
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 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

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-Te1/1/1)#lldp dcbx port-role auto-up
```

This example configures an FCoE host facing port:

```
console(config-if-Te1/1/1)#lldp dcbx port-role auto-down
```

show lldp tlv-select

Use the `lldp tlv-select` command in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Syntax

```
show lldp tlv-select interface <all|interface-id>
```

Parameter Description

Parameter	Description
Interface-id	A valid physical interface specifier
all	All interfaces

Default Configuration

The default is to show the per interface TLV configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Examples

```
console# show lldp tlv-select interface te1/0/1
Interface      ETS Config  ETS Recommend  PFC  App Priority QCN
-----
te1/0/1        Yes         No             Yes  No         Yes
```

```
console# show lldp tlv-select interface all
Interface      ETS Config  ETS Recommend  PFC  App Priority QCN
-----
te1/0/1        Yes         No             Yes  No         Yes
te1/0/2        No          No             Yes  No         Yes
```

show lldp dcbx

Use the `show lldp dcbx` command in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Syntax

Show lldp dcbx [interface <all|interface-id <detail|status>>]

Parameter Description

Parameter	Description
interface-id	A valid physical 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

This command has no user guidelines.

Example #1

DCBX Status:

```
console# show lldp dcbx interface all status
```

Interface	Status	Role	Version	Config DCBX		DCBX Errors	Frame Dscrd	TLV
				Rx	Tx			
tel1/0/1 0	Enabled	Auto-up	CEE 1.06	Yes	32	37	0	
tel1/0/2 0	Enabled	Auto-up	IEEE		32	37	0	
tel2/0/1 0	Enabled	Auto-dn	CIN 1.0		32	37	0	
tel2/0/2 0	Enabled	Auto-dn	IEEE		32	37	0	
tel3/0/1 0	Enabled	Auto-dn	CIN 1.0		32	37	0	
tel3/0/2 0	Disabled	Manual	IEEE		0	0	0	

Example #2

DCBX not enabled:

```
console# show lldp dcbx interface tel1/0/1
```

```
Interface tel1/0/1
```

```
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 tel/0/1
Interface tel/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:

Type	Subtype	Max/Oper Version	En/Will/Adv
PFC(3)	000	000	Y/Y/Y
PG(2)	000	000	Y/Y/Y
APP(4)	000	000	Y/Y/Y

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

		Max/Oper	
Type	Subtype	Version	En/Will/Err
PFC(3)	000	000/000	Y/N/N
PG(2)	000	000/000	Y/N/N
APP(4)	000	000/000	Y/N/N

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)

Type	Application	Priority	Status
Ethernet	FC0E	3	Enabled
TCP/SCTP	860	4	Disabled
TCP/SCTP	3260	4	Disabled

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):

```
console# show lldp dcbx interface tel1/0/1
Interface tel1/0/1
  DCBX Admin Status:           Enabled
  Configured DCBX Version:     CIN 1.0
  Peer DCBX Version:          CEE 1.6
  Peer MAC: 00:23:24:A4:21:03
  Peer Description:           Cisco Nexus 5020 IOS Version
5.00
  Auto-configuration Port Role: Auto-upstream
  Peer Is Configuration Source: True
```

```
Error Counters:
  ETS Incompatible Configuration: 7
  PFC Incompatible Configuration: 0
  Disappearing Neighbor:         0
  Multiple Neighbors Detected:   0
```

Example #5

DCBX enabled – detailed view:

```
console# show lldp dcbx interface tel1/0/1 detail
Interface tel1/0/1
  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

ETS Recommendation (TX Enabled)

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 ETS Recommendation:

Traffic Class Bandwidth: 0:0 1:1 2:2 3:0 4:0 5:3 6:0 7:0

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
------	-------------	----------

Ethernet	FC0E	3
----------	------	---

TCP/SCTP	3260	4
----------	------	---

Enhanced Transmission Selection Commands

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 Config mode) or interface (Interface Config mode) to the default mapping.

Syntax

```
classofservice traffic-class-group <trafficclass> <traffic class group>
```

```
no classofservice traffic-class-group
```

Parameter Description

Parameter	Description
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 Config modes

User Guidelines

For a given Traffic Class, a value specified in Interface Config mode only affects a single interface, whereas a change in Global Config mode is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service mappings.

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.

```
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 Config 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
```

Parameter Description

Parameter	Description
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 Config modes

User Guidelines

This command specified in Interface Config mode only affects a single interface; whereas, the Global Config mode setting is applied to all interfaces. Interface configuration overrides the global configuration on the designated interface. The Interface Config 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 Config 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
```

Parameter Description

Parameter	Description
bw-0..7	The minimum percentage bandwidth to be reserved to the TCG. Range 0 to 100.

Default Configuration

The default minimum bandwidth for all TCGs is 0% (no minimum guarantee).

Command Mode

Global Config mode, Interface Config mode

User Guidelines

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on the 81xx 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).

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 Config 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
```

Parameter Description

Parameter	Description
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 Config mode, Interface Config mode

User Guidelines

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config 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 **tcg-id** values are ignored. Each **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 **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(config)# traffic-class-group strict 1 2
```

traffic-class-group weight

Use the `traffic-class-group weight` command in Global Config or Interface Config 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
```

Parameter Description

Parameter	Description
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 Config mode, Interface Config mode

User Guidelines

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config 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 in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Syntax

```
show classofservice traffic-class-group [<interface-id>]
```

Parameter Description

Parameter	Description
wp-n	The weight percentage. Range 0 to 100.

Default Configuration

The default is to show the global traffic class to group mapping.

Command Mode

Privileged EXEC mode

User Guidelines

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-class-group

Use the **show interfaces traffic-class-group** command in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Syntax

show interfaces traffic-class-group [<interface-id>]

Parameter Description

Parameter	Description
interface-id	A valid physical interface specifier.

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. 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:

Field	Description
Interface	Displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Traffic Class Group	The traffic class Group identifier.
Min-Bandwidth	The minimum transmission bandwidth, expressed as a percentage. A value of 0 means bandwidth is not guaranteed. This is a configured value.
Max-Bandwidth	The maximum transmission bandwidth g, 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.

Field	Description
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. Strict priority scheduler is to provide lower latency to the higher CoS classes of traffic. Weighted scheduling is a round robin mechanism with weights associated to each CoS class of traffic. This is a configured value.
Weight Percentage	The weight of the TCG used during non-strict scheduling.

Example

The following example demonstrates how to display the global traffic class group configuration:

```
s1# show interfaces traffic-class-group
```

Global Configuration

TCG Id	Min. Bandwidth	Max Bandwidth	Scheduler Type	Weight Percentage
-----	-----	-----	-----	-----
0	0	0	Strict	0
1	0	0	WDRR	50
2	0	0	WDRR	50

FIP Snooping Commands

NOTE: Fiber Channel over Ethernet (FCoE) commands are only supported on the PC8024 and PC8024F switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.

The FCoE Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance. FIP uses a separate EtherType from FCoE to enable the distinction of discovery, initialization, and maintenance traffic from other FCoE traffic. FIP frames (with one exception) are the standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are a maximum of 2240 bytes.

This document describes FIP snooping, which is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following recommendations in Annex C of FC_BB_5 Rev 2.00. This allows for:

- 1 Auto-configuration of Ethernet ACLs based on information in the Ethernet headers of FIP frames.
- 2 Emulation of FC point-to-point links within the DCB Ethernet network.
- 3 Enhanced FCoE security/robustness by preventing FCoE MAC spoofing.

The FIP Snooping Bridge solution in PowerConnect Dell 4.2 supports configuration-only of perimeter port role and FCF-facing port roles and is only intended for use at the edge of the switched network.

The role of FIP Snooping-enabled ports on the switch falls under one of the following types:

- 1 Perimeter or Edge port (connected directly to ENode).
- 2 FCF facing port (that receives traffic from FCFs targeted to the ENodes).

The default port role in an FCoE enabled VLAN is as a perimeter port. FCF facing ports must be configured by the user.

Setting Up FIP Snooping

Three steps are required to set up FIP snooping:

- 1 Enable FIP snooping

```
feature fip-snooping
```

- 2 Configure a VLAN and enable it for FIP Snooping. The example below sets up ports 1 through 16 (CNA connected ports) and port 24 (FCF connected port) to use VLAN 100 and enables VLAN 100 for FIP snooping.

```
vlan 100
```

```
fip-snooping enable
```

```
exit
```

```
interface range te1/0/1-16,te1/0/24
```

```
switchport mode general
```

```
switchport general allowed vlan add 100 tagged
```

```
exit
```

- 3 Set up the port roles. The example below configures ports 1-16 as CNA connected ports which will receive information from the FCF connected port and sets the FCF connected port as the configuration source.

```
interface te1/0/24
```

```
lldp dcbx port-role configuration-source
```

```
fip-snooping port-mode fcf
```

```
interface range te1/0/1-16
```

```
lldp dcbx port-role auto-down
```

```
exit
```

Commands in this Chapter

This chapter explains the following commands:

[feature fip-snooping](#)

[show fip-snooping fcf](#)

[fip-snooping enable](#)

[show fip-snooping sessions](#)

[fip-snooping fc-map](#)

[show fip-snooping statistics](#)

[fip-snooping port-mode](#)

[show fip-snooping vlan](#)

show fip-snooping	clear fip-snooping statistics
show fip-snooping enode	–

feature fip-snooping

Use the **feature fip-snooping** command in Global Configuration mode to globally enable Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. Use the **no** form of the command to return the settings to the default values and disable FIP snooping.

Use the **no** form of the command to globally disable FIP snooping. When FIP snooping is globally disabled, received FIP frames are forwarded or flooded using the normal multicast rules. In addition, other FIP snooping commands are not available until the FIP snooping feature is enabled.

Syntax

feature fip-snooping

no feature fip-snooping

Default Configuration

The default mode is off (FIP snooping feature is disabled).

Command Mode

Global Configuration mode

User Guidelines

When FIP snooping is disabled, received FIP frames are forwarded or flooded using the normal multicast rules.

When FIP snooping is enabled, FC-BB-5 Annex D ACLs are installed on the switch and FIP frames are snooped. FIP snooping will not allow FIP or Fiber Channel over Ethernet (FCoE) frames to be forwarded over a port until the port is operationally enabled for PFC. VLAN tagging must be enabled on the interface in order to carry the dot1p values through the network.

Example

The following example enables the FIP snooping feature.

```
s1(config)#feature fip-snooping
```

feature fip-snooping enable

Use the **feature fip-snooping** command in VLAN Configuration mode to enable snooping of FIP packets on the configured VLANs. FIP snooping is disabled on VLANs by default.

Use the **no** form of the command to return the mode to the default (off).

Syntax

```
feature fip-snooping enable
```

```
no feature fip-snooping enable
```

Default Configuration

The default mode is off (FIP snooping is disabled.)

Command Mode

VLAN Configuration

User Guidelines

Priority Flow Control (PFC) must be operationally enabled before FIP snooping can operate on an interface. VLAN tagging must be enabled on the interface in order to carry the dot1p value through the network.

This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Example

The following example enables FIP snooping on VLANs 2, 3,...8.

```
s1(config)#vlan 2-8
```

```
s1(config-vlan)#fip-snooping enable
```


fip-snooping fc-map

Use the `fip-snooping fc-map` command in VLAN Configuration mode to configure the FP-MAP value on a VLAN. The FC map value is used to help in securing the switch against misconfiguration.

Syntax

```
fip-snooping fc-map 0x0 – 0xffffffff
```

```
no fip-snooping fc-map
```

Parameter Description

Valid FC map values are in the range of 0x0 to 0xffffffff.

Default Configuration

The default FC map value is 0x0efc00.

Command Mode

VLAN Configuration mode

User Guidelines

When configured using fabric-provided MAC addresses, FCoE devices transmit frames containing the FC map value in the upper 24 bits. Only frames that match the configured FC map value are passed across the VLAN. Frames with MAC addresses that do not match the FC map value are discarded.

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example

The following example configures an FC map value of 0x100 on VLAN 208.

```
(config)# vlan 208
(config-vlan)# fip-snooping enable
(config-vlan)# fip-snooping fc-map 0x100
```

fip-snooping port-mode

To relay the FIP packets received from the hosts toward the Fibre Channel Fabric (FCF), the switch needs to know the interfaces to which the FCFs are connected. Use the **fip-snooping port-mode** command in Interface Configuration mode to configure the interface that is connected towards FCF. By default, an interface is configured to be a host-facing interface if it is not configured to be an FCF-facing interface.

Syntax

fip-snooping port-mode fcf

no fip-snooping port-mode

Parameter Description

Parameter	Description
FCF	Fibre Channel Fabric

Default Configuration

The default behavior is configuration as a host-facing interface.

Command Mode

Interface (physical interface and port channel) Configuration

User Guidelines

It is recommended that FCF-facing ports be placed into auto-upstream mode in order to receive DCBX information and propagate it to the CNAs on the downstream (host-facing) ports.

Interfaces enabled for PFC should be configured in trunk or general mode and must be PFC-operationally enabled before FCoE traffic can pass over the port.

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example

The following example configures an interface to be connected to an FCF switch.

```
(config)# interface te1/0/1
(config-vlan)# fip-snooping port-mode fcf
```

show fip-snooping

Use the **show fip-snooping sessions** command in User EXEC or Privileged EXEC mode to display information about the global FIP snooping configuration and status.

Syntax

```
show fip-snooping
```

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following information is displayed.

Parameter	Description
Global Mode	FIP snooping configuration status on the switch. It displays Enable when FIP snooping is enabled on the switch and Disable when FIP snooping is disabled on the switch.
FCoE VLAN List	List of VLAN IDs on which FIP snooping is enabled.
FCFs	Number of FCFs discovered on the switch.
ENodes	Number of Enodes discovered on the switch.
Sessions	Total virtual sessions on the switch.

Parameter	Description
Max VLANs	Maximum number of VLANs that can be enabled for FIP snooping on the switch.
Max FCFs in VLAN	Maximum number of FCFs supported in a VLAN.
Max ENodes	Maximum number of ENodes supported in the switch.
Max Sessions	Maximum number of Sessions supported in the switch.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC or Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
(switch)# show fip-snooping
```

```
Global Mode:    Enable
FCoE VLAN List :  2,4,5-8
FCFs:          2
ENodes:        2
Sessions:      10
Max VLANs:     8
Max FCFs in VLAN:  4
Max ENodes:    312
Max Sessions:  1024
```

show fip-snooping enode

Use the **show fip-snooping enode** command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to ENodes.

Syntax

show fip-snooping enode [enode-mac]

Parameter Description

Parameter	Description
enode-mac	MAC address of the enode to display.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following information is displayed.

Parameter	Description
Interface	Interface to which the ENode is connected.
VLAN	ID number of the VLAN to which the ENode belongs.
NameID	Name of the ENode.
FIP-MAC	MAC address of the ENode.
FCID	Fiber channel ID number of the virtual port that was created by FCF when the ENode logged into the network.
Sessions Established	Number of successful virtual connections established.

The following additional information is displayed when the optional argument is supplied.

Parameter	Description
Sessions Waiting	Number of virtual connections waiting for FCF acceptance.
Sessions Failed	Number of virtual sessions failed.
Max-FCoE-PDU	Maximum FCoE PDU size the ENode MAC intends to use for FCoE traffic. This is equivalent to the maximum Ethernet frame payload the ENode intends to send.
Time elapsed	Time elapsed since first successful login session snooped from the ENode.

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example #1

The following example displays sample output of the command with no optional argument supplied.

```
(switch)# show fip-snooping enode
```

```
Interface  VLAN  Name-ID          ENode-MAC      FCFs
Sessions
```

```
-----
1/0/2      1      00000000        00:0c:29:65:82:bc  1
3
```

```
1/0/5      100    00000000        00:0d:31:23:53:11  2
5
```

Example #2

The sample output of the command below displays with the optional argument supplied.

```
(switch)# show fip-snooping enode 00:0c:29:65:82:bc
```

```
Interface  1/0/2
```

```
VLAN      1
```

```
Name-ID      000000
ENode-MAC   00:0c:29:65:82:bc
FCFs Connected1
Sessions Established3
Sessions Waiting 1
Session Failed 0
Max-FCoE-PDU 2158
Time elapsed 0 days, 1 hours, 20 minutes
```

show fip-snooping fcf

Use the `show fip-snooping fcf` command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to FCFs.

Syntax

```
show fip-snooping fcf [fcf-mac]
```

Parameter Description

Parameter	Description
fcf-mac	MAC address of the FCF.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following information is displayed when no FCF mac argument is supplied.

Parameter	Description
Interface	Interface to which the FCF is connected.
VLAN	ID number of the VLAN to which the FCF belongs.
No. of ENodes	Total number of ENodes that are connected to the FCF.
FPMA/SPMA	Type of the MAC address for ENode as negotiated by the FCF.
FCMAP	FCMAP value used by the FCF.
FCF-MAC	MAC address of the FCF.
Fabric Name	Name of the FCF.

Below is additional information regarding the FCF that is displayed when the optional FCF MAC address argument is provided.

Parameter	Description
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
D-bit	This reflects the value of the D-bit provided by the most recently received Discovery Advertisement from the FCF. When D-bit value is zero then FIP snooping bridge verifies the periodic VN_Port FIP Keep Alive frames associated with FCF and Discovery Advertisements sent by FCF. When D-bit is set to 1, switch discards snooped VN_Port FIP Keep Alive frames associated with FCF and does not timeout the FCoE sessions established with the FCF based on $FKA_VN_PERIOD * 5$ interval.
Available for Login	This reflects the value of the A bit provided by the most recently received Discovery Advertisement from the FCF. This provides the information that the transmitting FCF is available for FIP FLOGI/FDISC from ENodes. This is informational and shall have no effect on existing logins.
Priority	The Priority returned from the FCF in the Solicited Discovery Advertisement. This indicates the Priority that has been manually assigned to the FCF.

Parameter	Description
FKA-ADV	FIP keepalive interval (FKA_ADV_PERIOD) in seconds configured on the FCF multiplied by five. For example, if the FKA_ADV period configured on the FCF is 80 seconds, the value of this field is 400.
FCF Expiry Time	This is timer value to monitor the status of the FCF. FCF entry and all its associated virtual sessions will be removed when the value reaches 0. This value is reset to Configured FKA-ADV every time a Discovery Advertisement is received from the FCF-MAC.
Time Elapsed	Time since FCF is Discovered.

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example #1

The following displays sample output of the command when no optional argument is provided.

```
(config)# show fip-snooping fcf
```

```
-----
-----
Interface VLAN ENodes FPMA/ FC-MAP          FCF-MAC
Name-ID      Fabric-Name
              SPMA
-----
-----1/0/11      1    2          FPMA
0e:fc:00 00:0d:ec:b2:2c:80 20:65:00:0d: 20:65:00:0d:

ec:b1:9e:81  ec:97:52:c1

3/0/10      1    1          FPMA 0e:fc:00 00:0d:ec:b2:2c:81
00000000      00000000

3/0/15      100  1          FPMA 0e:fc:10 00:0c:ab:2c:eb:12
00000000      00000000
```

Example #2

The following displays sample output of the command when the optional argument is provided.

```
(switch)# show fip-snooping fcf 00:0d:ec:b2:2c:81
Interface 3/0/10
VLAN1
ENodes 1
FPMA/SPMAFPMA
FCF-MAC00:0d:ec:b2:2c:81
FC-MAP0e:fc:00
Name-ID20:65:00:0d:ec:b1:9e:81
Fabric-Name 20:65:00:0d:ec:97:52:c1
Sessions3
D-bit0
Available for Login1
Priority2
FKA-ADV(FKA_ADV_PERIOD*5) 250
FCF Expiry Time219
Time Elapsed0 days, 2 hours, 8 minutes
```

show fip-snooping sessions

Use the `show fip-snooping sessions` command in User EXEC or Privileged EXEC mode to display information about the active FIP snooping sessions.

Syntax

```
show fip-snooping sessions [[[vlan <vlan-d>] | [interface <interface-id>]
| [fcf <fcf-mac> [enode <enode-mac>]]] [detail]]
```

Parameter Description

Parameter	Description
Interface-id	ID of an interface on which FIP snooping has been enabled.
FCF-MAC	MAC address of the FCF that is part of the session.
ENode-MAC	MAC address of the ENode that is part of the session.
VLAN	ID number of the VLAN that contains the session.
FCoE MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
FC-ID	Fiber Channel ID of the virtual port that was created by the FCF when the ENode VN_Port did a FLOGI/NPIV/FDISC request.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

The following information is displayed:

Parameter	Description
FCF-MAC	MAC address of the FCF that is part of the session.
ENode-MAC	MAC address of the ENode that is part of the session.
VLAN	ID number of the VLAN that contains the session.
FCoE MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
FC-ID	Fiber Channel ID of the virtual port that was created by the FCF when the ENode logged into the network.

The command output format is different when the **detail** option is used. The information below is displayed.

Parameter	Description
VLAN	VLAN to which the session belongs.
FC-MAP	FCMAP value used by the FCF.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.
FCF Information	
Interface	Interface on which the FCF is discovered.
MAC	MAC address of the FCF.
ENodes	Total number of ENodes that are connected to the FCF.
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
ENode Information	
Interface	Interface to which the ENode is connected.
MAC	MAC address of the ENode.
Sessions	Total number of virtual sessions originated from ENodes to FCF in the VLAN.
Waiting	Total number of virtual connections waiting for FCF acceptance in the VLAN.
Session Information	
FCoE-MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
Request (FP, SP)	FIP session request type sent by ENode. This can be FLOGI or FDESC (NPIV FDISC). Whereas FP and SP values are the FP bit and the SP bit values in the FLOGI or NPIV FDISC request respectively.

Parameter	Description
Expiry Time	This is virtual connection/session expiry interval. This is used to monitor the status of the session. Session entry is removed when the value reaches 0. This value is reset to 450 secs (5*90 secs) every time an associated VN_Port FKA is received from the ENode. This is ignored (marked as NA) if the D-bit is set to one in the FCF Discovery Advertisements.
Mode	This is the addressing mode in use by the VN_Port at ENode. In other words, this is the type of MAC address granted (selected and returned) by FCF. This can be one of the addressing modes, i.e. FPMA or SPMA.
State	This is the state of the virtual session. The state is displayed as Tentative during the process of ENode login to FCF (using FLOGI or FDESC). It displays Active after ENode and FCF establish a successful virtual connection.
Session-Time	Time elapsed after this successful virtual session is established by ENode with FCF. The value is displayed in xd, yh, zm format where x represents number of days, y represents hours and z represents minutes elapsed following this successful virtual session. This field has no useful information for waiting sessions.

This command can only be entered after FIP snooping is enabled using the feature **fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Example #1

The following sample command output displays when no arguments are provided.

```
(switch)# show fip-snooping sessions
```

```
-----
-----
          FCF-MAC                ENode-MAC        VLAN        FCoE-
MAC          FC-ID
-----
-----
```

00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:00	38:0f:db	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:01	38:0f:dc	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:02	38:0f:dd	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:05	38:0f:e1	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:07	38:0f:e3	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:10	38:0f:e6	
00:0d:ec:b2:2c:80	00:0c:29:65:82:bc	100
0e:fc:00:ad:00:19	38:0f:ee	
00:0e:ad:12:23:53	00:0d:29:12:22:a6	200
0e:fc:11:aa:bb:00	44:23:a4	
00:0e:ad:12:23:53	00:0d:29:12:22:a6	200
0e:fc:11:aa:bb:01	44:02:ab	
00:0e:ad:12:23:53	00:0d:29:23:14:22	200
0e:fc:11:aa:bb:02	44:35:1b	
00:0e:ad:12:23:53	00:0d:29:23:14:22	200
0e:fc:11:aa:bb:03	44:35:2a	
00:0e:ad:12:23:53	00:0d:29:23:14:22	200
0e:fc:11:aa:bb:04	44:36:3b	

Example #2

The sample command output below displays when the detail option is specified.

```
(switch)# show fip-snooping sessions detail
```

VLAN: 100 FC-MAP: 0e:fc:00 FCFs: 1 ENodes:
1 Sessions: 7

<FCF Information>

Interface: 3/0/15 MAC: 00:0d:ec:b2:2c:80 ENodes:
1 Sessions: 7

<ENode Information>

Interface: 2/0/1 MAC: 00:0c:29:65:82:bc
Sessions: 7 Waiting: 0

<Session Information>

State	FCoE-MAC Session-Time	Request (FP, SP)	Expiry Time	Mode
ACTIVE	0e:fc:00:ad:00:00 0d, 04h, 20m	FLOGI (1,1)	200	FPMA
ACTIVE	0e:fc:00:ad:00:01 0d, 04h, 19m	FDESC (1,1)	259	FPMA
ACTIVE	0e:fc:00:ad:00:02 0d, 04h, 18m	FDESC (1,1)	215	FPMA
ACTIVE	0e:fc:00:ad:00:05 0d, 04h, 10m	FDESC (1,1)	231	FPMA
ACTIVE	0e:fc:00:ad:00:07 0d, 04h, 01m	FDESC (1,1)	189	FPMA
ACTIVE	0e:fc:00:ad:00:10 0d, 02h, 07m	FDESC (1,1)	210	FPMA
ACTIVE	0e:fc:00:ad:00:19 0d, 01h, 20m	FDESC (1,1)	222	FPMA

VLAN: 200 FC-MAP: 0e:fc:11 FCFs: 1 ENodes:
2 Sessions: 5

<FCF Information>

Interface: 3/0/11 MAC: 00:0e:ad:12:23:53 ENodes:
2 Sessions: 5

<ENode Information>

Interface: 1/0/10 MAC: 00:0d:29:12:22:a6
Sessions: 2 Waiting: 0

<Session Information>

FCoE-MAC	Request	Expiry	Mode	State
Session-Time		(FP,SP)	Time	
ACTIVE	0e:fc:11:ad:00:00	FLOGI(1,1)	242	FPMA
	0d, 02h, 30m			
ACTIVE	0e:fc:11:ad:00:01	FDESC(1,1)	245	FPMA
	0d, 02h, 28m			

<ENode Information>

Interface: 1/0/11 MAC: 00:0d:29:23:14:22
Sessions: 3 Waiting: 1

<Session Information>

FCoE-MAC	Request	Expiry	Mode	State
Session-Time		(FP,SP)	Time	
ACTIVE	0e:fc:11:ad:00:02	FLOGI(1,1)	202	FPMA
	0d, 02h, 20m			
ACTIVE	0e:fc:11:ad:00:03	FDESC(1,1)	228	FPMA
	0d, 01h, 18m			
ACTIVE	0e:fc:11:ad:00:03	FDESC(1,1)	232	FPMA
	0d, 01h, 02m			


```

----- FDESC (1,1) --- FPMA
TENTATIVE -----

```

Example #3

The sample command output below displays sessions between specified FCF and ENode.

```

(switch)# show fip-snooping sessions fcf
00:0e:ad:12:23:53 enode 00:0d:29:12:22:a6

```

```

-----
-----

```

FCF-MAC MAC	FC-ID FC-ID	ENode-MAC ENode-MAC	VLAN VLAN	FCoE- FCoE-
00:0e:ad:12:23:53		00:0d:29:12:22:a6	200	
0e:fc:11:aa:bb:00		44:23:a4		
00:0e:ad:12:23:53		00:0d:29:12:22:a6	200	
0e:fc:11:aa:bb:01		44:02:ab		

```

-----
-----

```

Example #4

The sample command output below displays sessions between specified FCF and ENode with the **detail** option.

```

(switch)# show fip-snooping sessions fcf
00:0e:ad:12:23:53 enode 00:0d:29:12:22:a6 detail

```

```

VLAN: 200   FC-MAP: 0e:fc:11           FCFs: 1   ENodes:
2   Sessions: 5

```

```

<FCF Information>

```

```
Interface: 3/0/11   MAC: 00:0e:ad:12:23:53  ENodes:
2   Sessions: 5
```

<ENode Information>

```
Interface: 1/0/10   MAC: 00:0d:29:12:22:a6
Sessions: 2   Waiting: 0
```

<Session Information>

FCoE-MAC	Request	Expiry	Mode	State
Session-Time		(FP,SP)	Time	
ACTIVE	0e:fc:11:ad:00:00	FLOGI (1,1)	242	FPMA
	0d, 02h, 30m			
ACTIVE	0e:fc:11:ad:00:01	FDESC (1,1)	245	FPMA
	0d, 02h, 28m			

show fip-snooping statistics

Use the `show fip-snooping statistics` command in User EXEC or Privileged EXEC mode to display the statistics of the FIP packets snooped in the VLAN or on an interface. If the optional (VLAN or interface) argument is not given, this command displays the statistics for all of the FIP snooping enabled VLANs.

Syntax

```
show fip-snooping statistics [vlan vlan-id] | [interface interface-id]
```

Parameter Description

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following table describes the packet counters per FIP Operation.

Packet Counter	Description
VR	Number of VLAN Request messages received on the VLAN.
VN	Number of VLAN Notification messages received on the VLAN.
MDS	Number of Multicast Discovery Solicitation messages snooped on the VLAN.
UDS	Number of Unicast Discovery Solicitation messages snooped on the VLAN.
FLOGI	Number of Fabric Logins snooped on the VLAN.
FDISC	Number of fabric discovery logins snooped on the VLAN.
LOGO	Number of Fabric Logouts on the VLAN.
VNPort-keep-alive	Number of VN_Port keepalive messages snooped on the VLAN.
MDA	Number of Multicast Discovery Advertisement messages snooped on the VLAN.
UDA	Number of Unicast Discovery Advertisement messages snooped on the VLAN.
FLOGI_ACC	Number of Fabric Logins accepted on the VLAN.
FLOGI_RJT	Number of Fabric Logins rejected on the VLAN.
FDISC_ACC	Number of Fabric Discoveries accepted on the VLAN.
FDISC_RJT	Number of Fabric Discoveries rejected on the VLAN.
LOGO_ACC	Number of Fabric Logouts accepted on the VLAN.
LOGO_RJT	Number of Fabric Logouts rejected on the VLAN.

Packet Counter	Description
CVL	Number of Clear Virtual Links actions on the VLAN.

The following table describes the other interface or session-related counters.

Other Counters	Description
Number of Virtual Session Timeouts	Number of Virtual sessions removed due to session timer expiry.
Number of FCF Session Timeouts	Number of ACTIVE sessions timed out due to Discovery Advertisements expiry from FCFs in the VLAN.
Number of Session configuration failures	Number of sessions in the VLAN that failed to be configured in the hardware.
Number of Sessions denied with FCF limit	Number of sessions that are denied to be created for the new FCF as the number of FCFs reached the maximum allowed in the VLAN.
Number of Sessions denied with ENode limit	Number of session create requests that are denied for the new ENode as the number of ENodes reached the maximum allowed in the system.
Number of Sessions denied with System limit	Number of sessions that are denied to be created as the number of sessions reached the maximum allowed in the system.

When an interface is provided as an argument, interface applicable statistics are only displayed. See [Example #3](#) below for applicable statistics on interface.

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example #1

Below is the sample command usage with no optional arguments supplied.

```
(switch)# show fip-snooping statistics
VLAN: 4
```

FIP-Operation	Number of Pkts
VR	2
VN	2
MDS	2
UDS	2
FLOGI	2
FDISC	2
LOGO	0
VNPort-keep-alive	200
MDA	25
UDA	2
FLOGI_ACC	2
FLOGI_RJT	0
FDISC_ACC	2
FDISC_RJT	0
LOGO_ACC	0
LOGO_RJT	0
CVL	0

Number of Virtual Session Timeouts:23
Number of FCF Session Timeouts: 6
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit: 10
Number of Sessions denied with ENode limit: 10
Number of Sessions denied with System limit: 12

VLAN: 200

```
-----
```

FIP-Operation	Number of Pkts
VR	2
VN	2
MDS	5
UDS	4
FLOGI	5
FDISC	5
LOGO	1
VNPort-keep-alive	310
MDA	35
UDA	3
FLOGI_ACC	4
FLOGI_RJT	0
FDISC_ACC	15
FDISC_RJT	0
LOGO_ACC	1
LOGO_RJT	0
CVL	0

```
-----
```

Number of Virtual Session Timeouts:2

Number of FCF Session Timeouts: 0

Number of Session configuration failures: 10

```
Number of Sessions denied with FCF limit: 0
Number of Sessions denied with ENode limit: 0
Number of Sessions denied with System limit: 21
```

Example #2

Below is the sample command output with optional VLAN argument supplied.

```
(switch)# show fip-snooping statistics vlan 200
```

```
VLAN: 200
```

```
-----
FIP-Operation      Number of Pkts
-----
VR                  2
VN                  2
MDS                  5
UDS                  4
FLOGI                5
FDISC                5
LOGO                 1
VNPort-keep-alive 310
MDA                  35
UDA                  3
FLOGI_ACC            4
FLOGI_RJT            0
FDISC_ACC            15
```

```

FDISC_RJT          0
LOGO_ACC           1
LOGO_RJT           0
CVL                0

```

```
-----
```

```

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:  21

```

Example #3

Below is the sample command output with optional interface argument supplied.

```
(switch)# show fip-snooping statistics interface 1/0/5
```

```
-----
```

FIP-Operation	Number of Pkts
VR	2
VN	2
MDS	5
UDS	1
FLOGI	2


```

FDISC                5
LOGO                 1
VNPort-keep-alive  310
MDA                  35
UDA                  3
FLOGI_ACC            4
FLOGI_RJT            0
FDISC_ACC            15
FDISC_RJT            0
LOGO_ACC             1
LOGO_RJT             0
CVL                  0

```

```
-----
```

```

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit: 0
Number of Sessions denied with ENode limit: 0
Number of Sessions denied with System limit: 21

```

show fip-snooping vlan

Use the **show fip-snooping vlan** command in User EXEC or Privileged EXEC mode to display the FCoE VLANs information and, additionally, the FIP snooping port status when optional argument is specified.

Syntax

```
show fip-snooping vlan [vlan-id]
```

Parameter Description

Parameter	Description
vlan-id	A VLAN enabled for FIP snooping.
VLAN	VLAN in which FIP snooping is enabled/operational.
FC-MAP	FCoE mapped address prefix of the FCoE forwarder for the FCoE VLAN.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Example

```
console#show fip-snooping vlan 200
```

```
VLAN:                200
FC-MAP:              0E:FC:00
Number of FCFs discovered:  1
Number of ENodes discovered: 2
Total virtual sessions in VLAN: 3
Active Ports:
Te1/0/2, Te1/0/3, Te1/0/21
```

Inactive Ports:

clear fip-snooping statistics

Use the `clear fip-snooping statistics` command in User EXEC or Privileged EXEC mode to clear the FIP Snooping statistics in the supplied VLAN or on a supplied interface. If the optional (VLAN or interface) argument is not given, this command clears the statistics on all FIP snooping-enabled VLANs.

Syntax

`clear fip-snooping statistics [vlan vlan-id] | [interface interface-id]`

Parameter Description

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC

User Guidelines

This command can only be entered after FIP snooping is enabled using the [feature fip-snooping](#) command. Otherwise, it does not appear in the CLI syntax tree.

Priority Flow Control Commands

NOTE: Fiber Channel over Ethernet (FCoE) commands are only supported on the PC8024 and PC8024F switches. CLI commands and Dell OpenManage Switch Administrator pages are not available for other switch models.

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 802.1Qbb 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 802.1Qbb.

Commands in this Chapter

This chapter explains the following commands:

[priority-flow-control mode](#)

[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 Config 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

Parameter Description

Parameter	Description
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 Config mode

User Guidelines

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 dot1p value through the network. Additionally, the dot1mapping to class-of-service must be set to one-to-one.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled.

Example

The following example enables PFC on an interface.

```
s1(config)#interface te1/0/1
s1(config-if-Te1/0/1)#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 Config 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
```

Parameter Description

Parameter	Description
drop	Disable lossless behavior on the selected priorities.
no-drop	Enable lossless behavior on the selected priorities.

Default Configuration

The default behavior for all priorities is drop.

Command Mode

Datacenter-Bridging Config mode

User Guidelines

The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

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 in Privileged EXEC mode to display the global or interface priority flow control status and statistics.

Syntax

`show interfaces interface-id priority-flow-control`

Parameter Description

This command uses an optional interface parameter.

Parameter	Description
interface-id	A valid Ethernet port identifier.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

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
```

```
Priority Received PFC Frames   Transmitted PFC Frames
-----
```

```

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

```

```
console#show interfaces priority-flow-control
```

Port	Drop Priorities	No-Drop Priorities	Operational Status
-----	-----	-----	-----
Te1/0/1	0-2,4-7	3	Active
Te1/0/2	0-2,4-7	3	Active
Te1/0/3	0-7		Inactive
Te1/0/4	0-7		Inactive
Te1/0/5	0-7		Inactive
Te1/0/6	0-7		Inactive
Te1/0/7	0-7		Inactive
Te1/0/8	0-7		Inactive
Te1/0/9	0-7		Inactive
Te1/0/10	0-7		Inactive
Te1/0/11	0-7		Inactive
Te1/0/12	0-7		Inactive

Te1/0/13	0-7		Inactive
Te1/0/14	0-7		Inactive
Te1/0/15	0-7		Inactive
Te1/0/16	0-7		Inactive
Te1/0/17	0-7		Inactive
Te1/0/18	0-7		Inactive
Te1/0/19	0-7		Inactive
--More-- or (q)uit			
Te1/0/20	0-7		Inactive
Te1/0/21	0-7		Inactive
Te1/0/22	0-7		Inactive
Te1/0/23	0-2,4-7	3	Active
Te1/0/24	0-7		Inactive

Layer 3 Commands

The chapters that follow describe commands that conform to the OSI model's Network Layer (Layer 3). Layer 3 commands perform a series of exchanges over various data links to deliver data between any two nodes in a network. These commands define the addressing and routing structure of the Internet.

This section of the document contains the following Layer 3 topics:

ARP Commands	Loopback Interface Commands
DHCP Server and Relay Agent Commands	Multicast Commands
DHCPv6 Commands	IPv6 Multicast Commands
DVMRP Commands	OSPF Commands
–	OSPFv3 Commands
IGMP Commands	Router Discovery Protocol Commands
IGMP Proxy Commands	Routing Information Protocol Commands
IP Helper/DHCP Relay Commands	Tunnel Interface Commands
IP Routing Commands	Virtual Router Redundancy Protocol Commands
IPv6 Routing Commands	–

ARP Commands

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 Chapter

This chapter explains the following commands:

arp	clear arp-cache
arp cachesize	clear arp-cache management
arp purge	ip local-proxy-arp
arp resptime	ip proxy-arp
arp retries	show arp
arp timeout	—

arp

Use the **arp** command in Global Configuration mode to create an Address Resolution Protocol (ARP) entry. Use the **no** form of the command to remove the entry.

Syntax

`arp ip-address hardware-address`

`no arp ip-address`

- *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.

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 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 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. The range is 256–1024384–4096.

Default Configuration

The default value is 10244096.

Command Mode

Global Configuration mode

User Guidelines

The ARP cache size is dependant on the switching hardware used. Values different from the default given above may exist in a given switch model.

Example

The following example defines an arp cachesize of 500.

```
console(config)#arp cachesize 500
```

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 disabled.

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, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, 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, 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. 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.

Example

```
console#configure
console(config)#arp dynamicrenew
console(config)#no arp dynamicrenew
```

arp purge

Use the **arp purge** command in Privileged EXEC mode 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.

Syntax

arp purge *ip-address*

- *ip-address* — The IP address to be removed from ARP 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 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 ageout time. Use the **no** form of the command to set the ageout time to the default.

Syntax

arp timeout *integer*

no arp timeout

- *integer*— The IP ARP entry ageout 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 in Privileged EXEC mode to remove all ARP entries of type dynamic from the ARP cache.

Syntax

```
clear arp-cache [gateway]
```

- `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

This command has no user guidelines.

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
```

IP Address	MAC Address	Interface	Type	Age
10.27.20.241	001A.A0FF.F662	Management	Dynamic	n/a
10.27.20.243	0019.B9D1.29A3	Management	Dynamic	n/a

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.

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

Interface Configuration (VLAN) mode

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 in Privileged EXEC mode 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 [brief]
```

- `brief` — Display ARP parameters.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC and Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

The show arp command will display static (user-configured) ARP entries regardless of whether they are reachable over an interface or not.

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 InterfaceType Age
-----
1.1.1.1.30000.0000.0022n/a Static n/a
```

DHCP Server and Relay Agent Commands

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 back in 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 Chapter

This chapter explains the following commands:

<code>ip dhcp pool</code>	<code>dns-server</code> (IP DHCP Pool Config)	<code>ip dhcp ping packets</code>	<code>service dhcp</code>
<code>bootfile</code>	<code>domain-name</code> (IP DHCP Pool Config)	<code>lease</code>	<code>sntp</code>
<code>clear ip dhcp binding</code>	<code>hardware-address</code>	<code>netbios-name-server</code>	<code>show ip dhcp binding</code>
<code>clear ip dhcp conflict</code>	<code>host</code>	<code>netbios-node-type</code>	<code>show ip dhcp conflict</code>
<code>client-identifier</code>	<code>ip dhcp bootp automatic</code>	<code>network</code>	<code>show ip dhcp global configuration</code>
<code>client-name</code>	<code>ip dhcp conflict logging</code>	<code>next-server</code>	<code>show ip dhcp pool</code>
<code>default-router</code>	<code>ip dhcp excluded-address</code>	<code>option</code>	<code>show ip dhcp server statistics</code>

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]
```

Parameter Description

Parameter	Description
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

PowerConnect 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#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)#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
```

Parameter Description

Parameter	Description
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 ntlldr
```

clear ip dhcp binding

Use the `clear ip dhcp binding` command in Privileged EXEC mode to remove automatic DHCP server bindings.

Syntax

```
clear ip dhcp binding {ip-address | *}
```

Parameter Description

Parameter	Description
*	Clear all automatic dhcp bindings.
ip-address	Clear a specific binding.

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 in Privileged EXEC mode 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 | *}
```

Parameter Description

Parameter	Description
*	Clear all dhcp conflicts.
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

Parameter Description

Parameter	Description
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)#client-identifier 01:03:13:18:22:33:11
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

client-name *name*

no client-name

Parameter Description

Parameter	Description
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.

Example

```
console(config-dhcp-pool)#client-identifier 01:03:13:18:22:33:11
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

```
default-router {ip-address1}[ip address2]
no default-router
```

Parameter Description

Parameter	Description
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
```

Parameter Description

Parameter	Description
<i>ip-address1</i>	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

Parameter Description

Parameter	Description
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 XX 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
```

Parameter Description

Parameter	Description
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
```

Parameter Description

This command does not require a parameter description.

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
```

Parameter Description

This command does not require a parameter description.

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}
```

Parameter Description

Parameter	Description
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
```

Parameter Description

Parameter	Description
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

```
lease {days[hours][minutes] | infinite}
```

```
no lease
```

Parameter Description

Parameter	Description
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 does not expire.

Default Configuration

The default is a 1 day lease.

Command Mode

DHCP Pool Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-dhcp-pool)#lease 1 12 59
```

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
```

Parameter Description

Parameter	Description
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 (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

```
netbios-node-type type
```

```
no netbios-node-type
```

Parameter Description

Parameter	Description
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 (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]
```

Parameter Description

Parameter	Description
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
```

Parameter Description

Parameter	Description
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

```
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

```
option code {ascii string1 | hex[string1...string8] | ip[ip-address1...ip-address8]}
```

```
no option code
```

Parameter Description

Parameter	Description
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.

Figure 46-1 lists the options that can be configured and their fixed length, minimum length, and length multiple requirements.

Figure 46-1. Option Codes and Lengths

Option Code	Fixed Length	Minimum Length	Multiple Of
2 (Time Offset)	4	–	–
4 (Time Server)	–	4	4
7 (Log Server)	–	4	4
8 (Cookie Server)	–	4	4
9 (LPR Server)	–	4	4

Figure 46-1. Option Codes and Lengths (continued)

Option Code	Fixed Length	Minimum Length	Multiple Of
10 (Impress Server)	–	4	4
11 (Resource Location Server)	–	4	4
12 (Host Name)	–	1	–
13 (Boot File Size)	2	–	–
14 (Merit File Dump)	–	1	–
16 (Swap Server)	4	–	–
17 (Root Path)	–	1	–
18 (Extensions Path)	–	1	–
19 (IP Forwarding Enable)	1	–	–
20 (Non-local Source Routing)	1	–	–
21 (Policy Filter)	–	8	8
22 (Max Datagram Reassembly)	2	–	–
23 (IP TTL)	1	–	–
24 (Path MTU Aging)	4	–	–
25 (Path MTU Plateau)	–	2	2
26 (Interface MTU)	2	–	–
27 (Subnets are local)	1	–	–
28 (Broadcast Address)	4	–	–
29 (Perform Mask)	1	–	–
30 (Mask Supplier)	1	–	–
31 (Perform Router Discovery)	1	–	–
32 (Router Solicitation Address)	4	–	–
33 (Static Router Option)	–	8	8

Figure 46-1. Option Codes and Lengths (continued)

Option Code	Fixed Length	Minimum Length	Multiple Of
34 (Trailer Encapsulation)	1	–	–
35 (ARP Cache Timeout)	4	–	–
36 (Ethernet Encapsulation)	1	–	–
37 (TCP TTL)	1	–	–
38 (TCP Keepalive Interval)	4	–	–
39 (TCP Keepalive Garbage)	1	–	–
40 (Network Information Service)	–	1	–
41 (Network Information Servers)	–	4	4
42 (NTP Servers)	–	4	4
43 (Vendor Specific Information)	1	–	–
45 (NetBIOS Datagram Distribution)	–	4	4
47 (Netbois Scope)	–	1	–
48 (X-Windows Font Server)	–	4	4
49 (X-Windows Display Manager)	–	4	4
58 (Renewal Time T1)	4	–	–
59 (Rebinding Time T2)	4	–	–
60 (Vendor Class)	–	1	–
64 (NIS Domain)	–	1	–
65 (NIS Servers)	–	4	4
66 (TFTP Server)	–	1	–

Figure 46-1. Option Codes and Lengths (continued)

Option Code	Fixed Length	Minimum Length	Multiple Of
68 (Mobile IP Home Agent)	–	0	4
69 (SMTP Server)	–	4	4
70 (POP3 Server)	–	4	4
71 (NNTP Server)	–	4	4
72 (WWW Server)	–	4	4
73 (Finger Server)	–	4	4
74 (IRC Server)	–	4	4
75 (Streetwork Server)	–	4	4
76 (STDA Server)	–	4	4

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 "ntpserver.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 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

Parameter Description

Parameter	Description
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(config-dhcp-pool)#sntp 192.168.21.2
```

show ip dhcp binding

Use the `show ip dhcp binding` command in Privileged EXEC mode to display the configured DHCP bindings.

Syntax

```
show ip dhcp binding [address]
```

Parameter Description

Parameter	Description
address	A valid IPv4 address

Default Configuration

The command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
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
```

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]
```

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

show ip dhcp global configuration

Use the `show ip dhcp global configuration` command in Privileged EXEC mode to display the DHCP global configuration.

Syntax

```
show ip dhcp server statistics
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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]
```

Parameter Description

Parameter	Description
poolname	Name of the pool. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

show ip dhcp server statistics

Use the `show ip dhcp server statistics` command in Privileged EXEC mode to display the DHCP server binding and message counters.

Syntax

```
show ip dhcp server statistics
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip dhcp server statistics
Automatic Bindings..... 100
Expired Bindings..... 32
Malformed Bindings..... 0

Messages                               Received
-----                               -
DHCP DISCOVER..... 132
```


DHCP REQUEST.....	132
DHCP DECLINE.....	0
DHCP RELEASE.....	32
DHCP INFORM.....	0

Messages	Sent
-----	-----
DHCP OFFER.....	132
DHCP ACK.....	132
DHCP NACK.....	0

DHCPv6 Commands

This chapter explains the following commands:

<code>clear ipv6 dhcp</code>	<code>service dhcpv6</code>
<code>dns-server (IPv6 DHCP Pool Config)</code>	<code>show ipv6 dhcp</code>
<code>domain-name (IPv6 DHCP Pool Config)</code>	<code>show ipv6 dhcp binding</code>
<code>ipv6 dhcp pool</code>	<code>show ipv6 dhcp interface (User EXEC)</code>
<code>ipv6 dhcp relay</code>	<code>show ipv6 dhcp interface (Privileged EXEC)</code>
<code>ipv6 dhcp server</code>	<code>show ipv6 dhcp pool</code>
<code>prefix-delegation</code>	<code>show ipv6 dhcp statistics</code>

clear ipv6 dhcp

Use the `clear ipv6 dhcp` command in Privileged EXEC mode 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
```

Parameter Description

Parameter	Description
<i>ipv6-address</i>	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

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)#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” sub-option 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

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(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** — Is 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

An IP interface (VLAN) can be configured in DHCP relay mode or DHCP server mode. Configuring an interface in DHCP server mode overwrites the DHCP relay mode configuration and vice-versa.

An interface in server mode cannot be configured as a DHCP client (ip address dhcp).

Example

The following example configures DHCPv6 server functionality.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 dhcp server pool
```

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
```


Parameter Description

Parameter	Description
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, <code>console (config) #snmp-server host "host name"</code>
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 (config) #ipv6 dhcp pool addrpool
console (config-dhcp6s-pool) #prefix-delegation
2020:1::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 (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

This command has no user guidelines.

Example

The following example enables DHCPv6 globally.

```
console#configure
console(config)#service dhcpv6
console(config)#no service dhcpv6
```

show ipv6 dhcp

Use the `show ipv6 dhcp` command in Privileged EXEC mode to display the DHCPv6 server name and status.

Syntax

```
show ipv6 dhcp
```

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the configured DHCP pool based on the entered IPv6 address.

```
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 [type number] [statistics]
```

Syntax Description

Parameter	Description
type number	Tunnel tunnel-id (Range: 0-7) or VLAN vlan-id (Valid VLAN id)
statistics	Enables statistics display if interface is specified.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display configuration and status information about an IPv6 DHCP interface or all interfaces.

Syntax

```
show ipv6 dhcp interface [interface-id]{statistics}
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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.

Term	Description
Mode	Displays whether the specified interface is in Client, Relay, or Server mode.
State	State of the DHCPv6 Client on this interface. The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.
Server DUID	DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.
T1 Time	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.
T2 Time	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.

Term	Description
Interface IAID	An identifier for an identity association chosen by this Client.
Leased Address	The IPv6 address leased by the DHCPv6 Server for this interface.
Preferred Lifetime	The preferred life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.
Valid Lifetime	The valid life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.
Renew Time	The time remaining (in seconds) to send a DHCPv6 Renew request to DHCPv6 Server for the leased address.
Expiry Time	The time (in seconds) when the DHCPv6 leased address expires.

Example

The following example shows the output from this command when the device has leased an IPv6 address from the DHCPv6 server on interface 1/0/1.



NOTE: Note that the interface is in client mode.

```

console#show ipv6 dhcp interface vlan 2
IPv6 Interface..... V12
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..... V110
Mode..... Relay
Relay Address.....
3030::3
Relay Interface Number..... Relay
Relay Remote ID.....
Option Flags.....

```

```
console#show ipv6 dhcp interface vlan 10
```

```

IPv6 Interface..... V110
Mode.....
Server
Pool Name..... asd

```

Server Preference..... 20
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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, Config mode and all Config sub-modes

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
```

DVMRP Commands

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 Chapter

This chapter explains the following commands:

<code>ip dvmrp</code>	<code>show ip dvmrp neighbor</code>
<code>ip dvmrp metric</code>	<code>show ip dvmrp nexthop</code>
<code>show ip dvmrp</code>	<code>show ip dvmrp prune</code>
<code>show ip dvmrp interface</code>	<code>show ip dvmrp route</code>

ip dvmrp

Use the `ip dvmrp` command to set the administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Syntax

```
ip dvmrp
no ip dvmrp
```

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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..... Disable
Version..... 3
Total Number of Routes..... 0
Reachable Routes..... 0
```

DVMRP INTERFACE STATUS

Interface	Interface Mode	Protocol State
-----	-----	-----

show ip dvmrp interface

Use the `show ip dvmrp interface` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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..... Disable
```

show ip dvmrp neighbor

Use the `show ip dvmrp neighbor` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the next hop information on outgoing interfaces for routing multicast datagrams.

```
console(config)#show ip dvmrp nexthop
```

Source IP	Source Mask	Interface	Type
-----	-----	-----	-----

show ip dvmrp prune

Use the `show ip dvmrp prune` command in Privileged EXEC mode 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, Config mode and all Config 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.

```
console(config)#show ip dvmrp prune
```

Group	IP Source	IP Source	Expir
Mask	Time (secs)		

show ip dvmrp route

Use the `show ip dvmrp route` command in Privileged EXEC mode to display the multicast routing information for DVMRP.

Syntax

`show ip dvmrp route`

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast routing information for DVMRP.

```
console#show ip dvmrp route
```

```
          Upstream                               Expiry
          Up Time
Source Address Neighbor Interface
Metric Time(secs) (secs)
```

IGMP Commands

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 PowerConnect 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 live (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.

Commands in this Chapter

This chapter explains the following commands:

<code>ip igmp</code>	<code>ip igmp version</code>
<code>ip igmp last-member-query-count</code>	<code>show ip igmp</code>
<code>ip igmp last-member-query-interval</code>	<code>show ip igmp groups</code>
<code>ip igmp query-interval</code>	<code>show ip igmp interface</code>
<code>ip igmp query-max-response-time</code>	<code>show ip igmp membership</code>
<code>ip igmp robustness</code>	<code>show ip igmp interface stats</code>
<code>ip igmp startup-query-count</code>	–
<code>ip igmp startup-query-interval</code>	–

ip igmp

Use the `ip igmp` command in Global Configuration mode to set the administrative mode of IGMP in the system to active. IGMP only operates over VLAN interfaces.

Syntax

```
ip igmp  
no ip igmp
```

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables IGMP.

```
console (config) #ip igmp
```

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#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 tenths`

`no ip igmp last-member-query-interval`

- *tenths* — 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(config)#interface vlan 15
console(config-if-vlan15)#ip igmp last-member-query-
interval 20
```

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.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip igmp query-max-response-time 10
```

ip igmp robustness

Use the `ip igmp robustness` command in Interface 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 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 in Privileged EXEC mode to display system-wide IGMP information.

Syntax

show ip igmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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]

Syntax Description

Parameter	Description
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 modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the registered multicast groups for VLAN 1.

```
console#show ip igmp groups interface vlan 3 detail
```

```
REGISTERED MULTICAST GROUP DETAILS
```

```
Version1  Version2  Group
Multicast      Last      Up      Expiry  Host
Host          Compat
IP Address      Reporter      Time      Time
Timer          Timer      Mode
-----
-----
```

```
225.0.0.5          1.1.1.5          00:00:05  00:04:15  -
-----          00:04:15  v2
```

show ip igmp interface

Use the `show ip igmp interface` command in Privileged EXEC mode to display the IGMP information for the specified interface.

Syntax

```
show ip igmp interface [interface-type interface-number]
```

Syntax Description

Parameter	Description
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 modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays IGMP information for VLAN 11.

```
console#show ip igmp 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 in Privileged EXEC mode 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 modes, Config mode and all Config sub-modes

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 interface 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, Config mode and all Config sub-modes

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

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.

PowerConnect supports IGMP Version 3, Version 2 and Version 1. Version 3 adds support for source filtering [SSM] and needs to be interoperable with Versions 1 and 2. Version 2 supports the group membership terminations to be quickly reported to overcome leave latency and is designed to be interoperable with Version 1.

Commands in this Chapter

This chapter explains the following commands:

<code>ip igmp-proxy</code>	<code>show ip igmp-proxy interface</code>
<code>ip igmp-proxy reset-status</code>	<code>show ip igmp-proxy groups</code>
<code>ip igmp-proxy unsolicited-report-interval</code>	<code>show ip igmp-proxy groups detail</code>
<code>show ip igmp-proxy</code>	—

ip igmp-proxy

Use the `ip igmp-proxy` command in Interface Configuration mode to enable the IGMP Proxy on the router. To enable the IGMP Proxy on the router, multicast forwarding must be enabled and there must be no multicast routing protocols enabled on the router.

Syntax

```
ip igmp-proxy
```

```
no ip igmp-proxy
```

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 IGMP Proxy on the VLAN 15 router.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy
```

ip igmp-proxy reset-status

Use the `ip igmp-proxy 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 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(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy reset-status
```

ip igmp-proxy unsolicited-report-interval

Use the `ip igmp-proxy unsolicited-report-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 unsolicited-report-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(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy unsolicited-
report-interval 10
```

show ip igmp-proxy

Use the `show ip igmp-proxy` command in Privileged EXEC mode 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`

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the host interface status parameters.

```
console#show ip igmp-proxy

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 interface

Use the `show ip igmp-proxy interface` command in Privileged EXEC mode 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 interface`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 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 groups` command in Privileged EXEC mode 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 groups`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 groups
```

```
Interface Index.....  
vlan13
```

Group State	Address Filter	Last Reporter Mode	Sources	Up Time	Member
-------------	----------------	--------------------	---------	---------	--------

225.0.1.1	MEMBER Exclude	13.13.13.1	0	7	DELAY-
-----------	----------------	------------	---	---	--------

```
225.0.1.2          13.13.13.1    48          DELAY-
MEMBER Exclude          0
```

show ip igmp-proxy groups detail

Use the `show ip igmp-proxy groups detail` command in Privileged EXEC mode to display complete information about multicast groups that IGMP Proxy has reported.

Syntax

```
show ip igmp-proxy groups detail
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays complete information about multicast groups that IGMP Proxy has reported.

```
console#show ip igmp-proxy groups detail
Interface Index.....
vlan13
Group Address  Last Reporter  Up Time  Member
State Filter Mode Sources
-----
-----
-----
225.0.1.1      13.13.13.1    26      DELAY-
MEMBER Exclude          0
```

225.0.1.2	13.13.13.1	67	DELAY-
MEMBER Exclude	0		

IP Helper/DHCP Relay Commands

The IP Helper feature provides the ability for a router to forward configured UDP broadcast packets to a particular IP address. 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 (with the limited broadcast address 255.255.255.255, or a network directed broadcast address).

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 relays 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 51-1](#).

Table 51-1. UDP Destination Ports

Protocol	UDP Port Number
IEN-116 Name Service	42

Protocol	UDP Port Number
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol	69

Certain preexisting configurable DHCP relay options do not apply to relay of other protocols. These options are unchanged. The user 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, 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 limited broadcast address (255.255.255.255) or a directed broadcast address for the receive 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.

DHCP relay cannot be enabled and disabled globally. IP helper can be enabled or disabled globally. Enabling IP helper enables DHCP relay.

Commands in this Chapter

This chapter explains the following commands:

<code>bootpdhcprelay maxhopcount</code>	<code>ip helper-address</code> (global configuration)
<code>bootpdhcprelay minwaittime</code>	<code>ip helper-address</code> (interface configuration)
<code>clear ip helper statistics</code>	<code>ip helper enable</code>
<code>ip dhcp relay information check</code>	<code>show ip helper-address</code>
<code>ip dhcp relay information check-reply</code>	<code>show ip dhcp relay</code>
<code>ip dhcp relay information option</code>	<code>show ip helper statistics</code>
<code>ip dhcp relay information option-insert</code>	—

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

User Guidelines

Enable DHCP Relay using the [ip helper enable](#) command.

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-sinceclient-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

User Guidelines

Enable DHCP Relay using the [ip helper enable](#) command.

Example

The following example defines a minimum wait time of 10 seconds.

```
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
```

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 ip helper statistics
```

ip dhcp relay information check

Use the `ip 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 sub-options.

Syntax

```
ip dhcp relay information check  
no ip dhcp relay information check
```

Parameter Description

This command has no arguments or keywords.

Default Configuration

This is enabled by default for a DHCP relay agent.

Command Mode

Global 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.

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 sub-options.

Syntax

```
ip dhcp relay information check-reply [none]
```

```
no ip dhcp relay information check-reply
```

Parameter Description

Parameter	Description
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(config)#interface vlan 10
console(config-if-vlan10)#ip dhcp relay information check
```

ip dhcp relay information option

Use the **ip dhcp relay information option** command in Global Configuration mode to enable 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 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

User Guidelines

Enable DHCP Relay using the `ip helper enable` command.

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 option insert configuration to the default.

Syntax

```
ip dhcp relay information option-insert [none]
```

```
no ip dhcp relay information option-insert
```

Parameter Description

Parameter	Description
none	Use to disable insertion of circuit id and remote agent id options into DHCP messages.

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.

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 0 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-rip** (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.

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.

The command `no ip helper-address` with no arguments clears all global IP helper addresses.

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 51-1](#)) to the server at 20.1.1.1, use the following commands:

```
console#config
console(config)#ip helper-address 20.1.1.1
```


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 0 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.

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#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#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 dns
```

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#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 2/6
console(config-if-vlan6)#ip helper-address
192.168.23.1 162
console(config-if-vlan6)#ip helper-address discard
dhcp
```

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.

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 [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`.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Field	Description
Interface	The relay configuration is applied to packets that arrive on this interface. This field is set to “any” for global IP helper entries.

UDP Port	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 51-1 .
Discard	If “Yes”, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Example

```
show ip helper-address
```

```
IP helper is enabled
```

```

Interface      UDP Port      Discard      Hit Count      Server Address
-----
      vlan 100          dhcp          No              10          10.100.1.254
                                     10          10.100.2.254
      vlan 101          any           Yes              2
      any              dhcp          No              0          10.200.1.254

```

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
```

Parameter Description

This command has no arguments or keywords.

Default Configuration

The command has no default configuration.

Command Mode

User EXEC and Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Field	Description
DHCP client messages received	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 > 1 and having valid source and destination IP addresses.
DHCP client messages relayed	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.
DHCP server messages received	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.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP client messages received	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.
UDP client messages relayed	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.
DHCP message hop count exceeded max	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.
DHCP message with secs field below min	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.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.

Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

Example

```
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

The Routing Module provides the base Layer 3 support for Local Area Network (LAN) and Wide Area Network (WAN) environments. The PowerConnect switches allows the network operator to build a complete Layer 3+ configuration with advanced functionality. As the PowerConnect defaults to Layer 2 switching functionality, routing must be explicitly enabled on the PowerConnect to perform Layer 3 forwarding. For PowerConnect 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 PowerConnect network 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 PowerConnect, 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 0.

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, PowerConnect 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, PowerConnect enables configuring a static reject route for that network on the router. Such traffic is discarded and the ICMP destination unreachable message is sent back to the source. Static reject routes are typically used to prevent routing loops.

Default Routes

PowerConnect 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.

Commands in this Chapter

This chapter explains the following commands:

encapsulation	show ip interface
ip address	show ip protocols
ip mtu	show ip route
ip netdirbcast	show ip route configured
ip route	show ip route connected
ip route default	show ip route preferences
ip route distance	show ip route summary
ip routing	show ip traffic
show ip brief	show ip vlan

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 address

Use the `ip address` command in Interface Configuration mode to configure an IP address on an interface. Also use this command to configure one or more secondary IP addresses on the interface. The `ip address none` command sets the IP address to **none**. The `no ip address` command sets the IP address to the default (whatever the default is). Use the `show ip interface` command to display the configured IP addresses.

Syntax

`ip address ip-address {subnet-mask | prefix-length} [secondary]`

`no ip address ip-address {subnet-mask | prefix-length} [secondary]`

- `ip-address` — IP address of the interface.
- `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

This command has no default configuration.

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.

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 mtu

Use the **ip mtu** command in Interface Configuration mode to set the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Packets forwarded in hardware ignore the IP MTU. Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the `ip mtu` command. 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).

Syntax

```
ip mtu [bytes]
no ip mtu
```

Parameter Description

Parameter	Description
<i>bytes</i>	Specifies the maximum transmission size of an IP frame. (Range: 68-9198)

Default Configuration

1500 bytes is the default configuration.

Command Mode

Interface Configuration (VLAN) mode, Global Configuration mode

User Guidelines

Using this command in Global Configuration mode sets the IP MTU for all routing VLANs. This setting is adjusted internally when the link MTU command is issued.

Example

The following example defines 1480 as the MTU for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip mtu 1480
```

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 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. 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.

Syntax

`ip route ip addr { subnetmask | prefix length } nextHopRtr [preference]`

`no ip route ip addr { subnetmask | prefix length } nextHopRtr [preference]`

- *ip-address* — IP address of destination interface.
- *subnet-mask* — Subnet mask of destination interface.
- *prefix-length* — Length of prefix. Must be preceded with a forward slash (/). (Range: 0-32 bits)
- *nextHopRtr* — 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 the static routes to be visible, you must:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Example

The following example identifies the *ip-address subnet-mask, next-hop-ip* and a preference value of 200.

```
console(config)#ip route 192.168.10.10 255.255.255.0  
192.168.20.1 metric 200
```

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.

Syntax

ip route default *next-hop-ip* [*preference*]

no ip route default *next-hop-ip* [*preference*]

- *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.

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.

Syntax

ip route distance *integer*

no ip route distance *integer*

- *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.

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

User Guidelines

Use the [show ip brief](#) command to determine if routing is enabled or disabled.

Example

The following example enables IPv4 and IPv6 routing for VLAN 15

```
console(config)#ip routing
```

show ip brief

Use the **show ip brief** command in Privileged EXEC mode to display all the summary information of the IP.

Syntax

show ip brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays IP summary information.

```
console#show ip brief
Default Time to Live..... 30
Routing Mode..... Disabled
IP Forwarding Mode..... Enabled
Maximum Next Hops..... 2
```

show ip interface

Use the **show ip interface** command in Privileged EXEC mode to display information about one or more IP interfaces. The output shows how each IP address was assigned.

Syntax

show ip interface [type number]

Syntax Description

Parameter	Description
type	Interface type (loopback, out-of-band, or vlan)

Parameter	Description
number	Interface number. Valid only for loopback and VLAN types.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

The Method field contains one of the following values.

Field	Description
DHCP	The address is leased from a DHCP server.
Manual	The address is manually configured.

ds

The following examples display all IP information and information specific to VLAN 2.

```
console#show ip interface
```

```
Default Gateway..... 0.0.0.0
```

```
Burned In MAC Address..... 001E.C9AA.AC84
```

Routing Interfaces:

```

Interface      State      IP Address      IP Mask
Method
-----
-----
Vl1            Down      0.0.0.0         0.0.0.0
None
```

The Method field contains one of the following values:

- DHCP — The address is leased from a DHCP server.
- Manual — The address is manually configured.

The **Method** field is also added to the long form.

```
console#show ip interface vlan2
```

```
Routing Interface Status..... Up
Primary IP Address.....192.168.75.1/255.255.255.0
Method..... DHCP
Routing Mode..... Enable
Administrative Mode..... Enable
Forward Net Directed Broadcasts.... Disable
Proxy ARP..... Enable
Local Proxy ARP..... Disable
Active State..... Active
Link Speed Data Rate..... 100 Half
MAC address..... 00:11:88:2A:3C:B3
Encapsulation Type..... Ethernet
IP MTU..... 1500
Bandwidth..... 100000 kbps
Destination Unreachables..... Enabled
ICMP Redirects..... Enabled
```

```
console#show ip interface out-of-band
```

```

IP Address..... 10.131.11.66
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.131.11.1
Configured IPv4 Protocol..... DHCP
Burned In MAC Address..... 001E.C9AA.AD1C

```

show ip protocols

Use the `show ip protocols` command in Privileged EXEC mode 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
```

Parameter Description

Parameter	Description
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.

Parameter	Description
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv2 Section	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or "route preference") for intra-area, inter-area, and external routes.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type to advertise for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.

Parameter	Description
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ASBR Status	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.
RIP Section	
RIP Admin Mode	Whether RIP is globally enabled.
Split Horizon Mode	Whether RIP advertises routes on the interface where they were received.
Default Metric	The metric assigned to redistributed routes.
Default Route Advertise	Whether this router is originating a default route.
Distance	The administrative distance for RIP routes.
Interface	The interfaces where RIP is enabled and the version sent and accepted on each interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following shows example CLI display output for the command.

```
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

Redist
Source      Metric      Metric Type      Subnets      Dist List
-----
static      default          2              Yes           None
connected   10              2              Yes           1

Number of Active Areas..... 3 (3 normal, 0
stub, 0 nssa)
ABR Status..... Yes
ASBR Status..... Yes

Routing Protocol..... RIP

```

```

RIP Admin Mode..... Enable
Split Horizon Mode..... Simple
Default Metric..... Not configured
Default Route Advertise..... Disable
Distance..... 120

```

```

Interface                Send          Recv
-----                -
0/25                    RIPv2        RIPv2

```

show ip route

Use the **show ip route** command in Privileged EXEC mode 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.

Syntax

```

show ip route [ip-address [mask | prefix-length] [longer-prefixes] | ospf | rip
| static]

```

Syntax Description

Parameter	Description
ip-address	Specifies the network for which the route is to be displayed and displays the best matching best-route for the address.
mask	Subnet mask of the IP address.
<i>prefix-length</i>	Length of prefix, in bits. Must be preceded with a forward slash (/). (Range: 0-32 bits.)
longer-prefixes	Indicates that the <i>ip-address</i> and <i>subnet-mask</i> pair becomes the prefix, and the command displays the routes to the addresses that match that prefix.
<i>ospf</i>	Show OSPF originated routes.
rip	Show RIP originated routes.

Parameter	Description
static	Show statically originated routes.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

- If the subnet mask is specified, then only routes with an exact match are displayed.
- If only an IP address is specified, the best route for the IP address is displayed.
- If the **longer-prefixes** option is specified, then the subnets within an aggregate are displayed.

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, 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 0.0.0.0/0 [254/0] via 10.1.20.1
C 10.1.20.0/24 [0/1] directly connected, V12
C 4.4.0.0/16 [0/1] directly connected, Lo1
C 20.1.20.0/24 [0/1] directly connected, V14

```

show ip route configured

Use the `show ip route configured` command in Privileged EXEC mode to display the configured routes, whether they are reachable or not.

Syntax

`show ip route configured`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip route configured
```

```
Route Codes: R - RIP Derived, O - OSPF Derived, C -  
Connected, S - Static
```

```
          B - BGP 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
```

```
Default Gateway is not configured
```

```
S          10.0.0.0/8 [1/0] via 1.2.3.5
```

show ip route connected

Use the `show ip route connected` command in Privileged EXEC mode display connected routes. Connected routes are those that are reachable over a switch interface.

Syntax

`show ip route connected`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip route connected
Route Codes: R - RIP Derived, O - OSPF Derived, C -
Connected, S - Static
B - BGP 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
IP Routing Commands 1009
Default Gateway is not configured
S 10.0.0.0/8 [1/0] via 1.2.3.5
```

show ip route preferences

Use the **show ip route preferences** command in Privileged EXEC mode displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

The user can configure a global default gateway using the **ip default-gateway** command, creating a default route with a preference of 253. The **show ip route preferences** command lists the new preference value. The **show** command also displays the preference of default routes learned from a DHCP server.

Syntax

```
show ip route preferences
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays IP route preferences.

```
console#show ip route preferences
```

```
Local..... 0
Static..... 1
OSPF Intra..... 110
OSPF Inter..... 110
OSPF External..... 110
```

RIP.....	120
Configured Default Gateway.....	253
DHCP Default Gateway.....	254

show ip route summary

Use the `show ip route summary` command in Privileged EXEC mode to display the routing table summary, including best and non-best routes.

Syntax

```
show ip route summary [best]
```

Parameter Description

Parameter	Description
best	Shows the number of best routes. To include the number of all routes, do not use this optional parameter.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the IP route summary.

```
console#show ip route summary
Connected Routes..... 0
Static Routes..... 0
RIP Routes..... 0
```


OSPF Routes.....	0
Intra Area Routes.....	0
Inter Area Routes.....	0
External Type-1 Routes.....	0
External Type-2 Routes.....	0
Total routes.....	0

show ip traffic

Use the **show ip traffic** command in User EXEC mode to display IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Syntax

```
show ip traffic
```

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
IcmpInSrcQuenchs.....	0
IcmpInRedirects.....	0
IcmpInEchos.....	3
IcmpInEchoReps.....	0

IcmpInTimestamps.....	0
IcmpInTimestampReps.....	0
IcmpInAddrMasks.....	0
IcmpInAddrMaskReps.....	0
IcmpOutMsgs.....	3
IcmpOutErrors.....	0
IcmpOutDestUnreachs.....	0
IcmpOutTimeExcds.....	0
IcmpOutParmProbs.....	0
IcmpOutSrcQuenchs.....	0
IcmpOutRedirects.....	0
IcmpOutEchos.....	3
IcmpOutEchoReps.....	3
IcmpOutTimestamps.....	0
IcmpOutTimestampReps.....	0
IcmpOutAddrMasks.....	0

show ip vlan

Use the **show ip vlan** command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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

IPv6 Routing Commands

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 Chapter

This chapter explains the following commands:

<code>clear ipv6 neighbors</code>	<code>ipv6 mld query-max-response-time</code>	<code>ipv6 route</code>	<code>show ipv6 mld-proxy groups detail</code>
<code>clear ipv6 statistics</code>	<code>ipv6 mld router</code>	<code>ipv6 route distance</code>	<code>show ipv6 mld-proxy interface</code>
<code>ipv6 address</code>	<code>ipv6 mtu</code>	<code>ipv6 unicast-routing</code>	<code>show ipv6 mld traffic</code>
<code>ipv6 enable</code>	<code>ipv6 nd dad attempts</code>	<code>ping ipv6</code>	<code>show ipv6 neighbors</code>
<code>ipv6 hop-limit</code>	<code>ipv6 nd managed-config-flag</code>	<code>ping ipv6 interface</code>	<code>show ipv6 route</code>
<code>ipv6 host</code>	<code>ipv6 nd ns-interval</code>	<code>show ipv6 brief</code>	<code>show ipv6 route preferences</code>

ipv6 mld last-member-query-count	ipv6 nd other-config-flag	show ipv6 interface	show ipv6 route summary
ipv6 mld last-member-query-interval	ipv6 nd prefix	show ipv6 interface management statistics	show ipv6 traffic
ipv6 mld-proxy	ipv6 nd ra-interval	show ipv6 mld groups	show ipv6 vlan
ipv6 mld-proxy reset-status	ipv6 nd ra-lifetime	show ipv6 mld interface	traceroute ipv6
ipv6 mld-proxy unsolicit-rprt-interval	ipv6 nd reachable-time	show ipv6 mld-proxy	–
ipv6 mld query-interval	ipv6 nd suppress-ra	show ipv6 mld-proxy groups	–

clear ipv6 neighbors

Use the **clear ipv6 neighbors** command in Privileged EXEC mode 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 in Privileged EXEC mode 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 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 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)#interface vlan 15
console(config-if-vlan15)#ipv6 enable
```

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
```

Parameter Description

Parameter	Description
count	The number of hops before the PDU expires (Range 0-255).

Default Configuration

The default count is 64 hops.

Command Mode

Global Configuration

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::/32
```

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-proxy

Use the `ipv6 mld-proxy` command to enable MLD Proxy on the router. To enable MLD Proxy on the router, you must also enable multicast forwarding. Also, ensure that there are no other multicast routing protocols enabled on the router. Use the “no” form of this command to disable MLD Proxy.

Syntax

```
ipv6 mld-proxy
```

```
no ipv6 mld-proxy
```

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-proxy
```

ipv6 mld-proxy reset-status

Use the `ipv6 mld-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-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-proxy reset-status
```

ipv6 mld-proxy unsolicit-rprt-interval

Use the `ipv6 mld-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-proxy unsolicited-report-interval interval
```

```
no ipv6 mld-proxy unsolicited-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-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 mld router

The `ipv6 mld router` command is used to enable MLD in the router in global configuration mode and for a specific interface in interface configuration mode. Use the “no” form of this command to disable MLD.

Syntax

```
ipv6 mld router
```

```
no ipv6 mld router
```

Default Configuration

MLD is disabled by default.

Command Mode

Global Configuration mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld router
```

ipv6 mtu

Use the **ipv6 mtu** command in Interface Configuration mode to set the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default MTU with a new MTU value. The IPv6 MTU is only observed for packets originating on the switch. Packets forwarded by the hardware ignore the IPv6 MTU.

Syntax

```
ipv6 mtu <bytes>
```

```
no ipv6 mtu
```

Parameter Description

Parameter	Description
<i>bytes</i>	The maximum transmission size of an IPv6 frame. (Range: 1280-1500)

Default Configuration

The default MTU is 1500.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 mtu 1300
```

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
```

Parameter Description

Parameter	Description
<i>value</i>	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 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(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 nd ns-interval 5000
```

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`

Syntax Description

Parameter	Description
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(config)#interface vlan 11
console(config-if-vlan11)#ipv6 nd prefix 2020:1::1/64
```

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
console(config-if-vlan15)#ipv6 nd reachable-time 5000
```

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 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*

Syntax Description

Parameter	Description
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 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.

```
console(config)#ipv6 route 2020:1::1/64 2030:1::2
```

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
```

ping ipv6

Use `ping ipv6` command in Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Syntax

`ping ipv6 {ip-address | hostname} [size size]`

- *ipv6-address* — Target IPv6 address to ping.
- *hostname* — Hostname to ping (contact). (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, `console(config)#ping ipv6 "host name"`
- *size* — Size of the datagram. (Range: 48–2048 bytes)

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 determines whether another computer is on the network at the IPv6 address specified.

```
console#ping ipv6 2030:1::1/64
```

```
Send count=3, Receive count=0 from 2030:1::1/64
```

```
Average round trip time = 0.00 ms
```

ping ipv6 interface

Use **ping ipv6 interface** command in the Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the **interface** keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. The source can be a loopback, tunnel, or logical interface.

Syntax

```
ping ipv6 interface {vlan vlan-id | tunnel tunnel-id} | loopback loopback-id link-local-address [size datagram-size]
```

- *vlan-id* — Valid VLAN ID.
- *tunnel-id* — Tunnel identifier. (Range: 0-7)
- *loopback-id* — Loopback identifier. (Range: 0-7)
- *link-local-address* — IPv6 address to ping.
- *datagram-size* — Size of the datagram. (Range: 48-2048 bytes)

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 determines whether another computer is on the network at the IPv6 address specified.

```
console(config)#ping ipv6 interface loopback 1
FE80::202:BCFF:FE00:3068/128

Send count=3, Receive count=0 from
FE80::202:BCFF:FE00:3068/128

Average round trip time = 0.00 ms
```

show ipv6 brief

Use the `show ipv6 brief` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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]]
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

The Method field contains one of the following values.

Field	Description
Auto	The IPv6 address is automatically generated using IPv6 auto address configuration (RFC 2462).

Field	Description
Config	The IPv6 address is manually configured.
DHCP	The IPv6 address is leased from a DHCP server.
TENT	Tentative address.

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
-----
VI3    Enabled FE80::211:88FF:FE2A:3E3C/128
        2033::211:88FF:FE2A:3E3C/64
VI5    Enabled FE80::211:88FF:FE2A:3E3C/128
        2017::A42A:26DB:1049:43DD/128           [DHCP]
VI7    Enabled FE80::211:88FF:FE2A:3E3C/128
        2001::211:88FF:FE2A:3E3C/64           [AUTO]
VI9    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

2017::A42A:26DB:1049:43DD/128 [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

Address DHCP Mode.....
Enabled

Router Advertisement NS Interval..... 0

Router Advertisement Lifetime..... 1800

Router Advertisement Reachable Time..... 0

Router Advertisement Interval..... 600

Router Advertisement Managed Config Flag.....
Disabled
```

```

Router Advertisement Other Config Flag.....
Disabled

Router Advertisement Router Preference.....
medium

Router Advertisement Suppress Flag.....
Disabled

IPv6 Destination Unreachables.....
Enabled

IPv6 Default Router.....
fe80::213:c4ff:fedb:6c42

```

show ipv6 interface management statistics

Use the `show ipv6 interface management statistics` command in Privileged EXEC mode to show the DHCPv6 client statistics.

Syntax

```
show ipv6 interface management statistics
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 interface management 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..... 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 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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed as a table when `vlan vlan-id` is specified:

Field	Description
Number of (*, G) entries	Displays the number of groups present in the MLD Table.
Number of (S, G) entries	Displays the number of include and exclude mode sources present in the MLD Table.
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Uptime	Time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table.

If `vlan vlan-id` is not specified, the following fields are displayed for each multicast group and each interface:

Field	Description
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Uptime	Time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table of this interface.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are INCLUDE and EXCLUDE.

Compatibility Mode	The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.
Version 1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.

The following table is displayed to indicate all the sources associated with this group:

Field	Description
Source Address	The IP address of the source.
Uptime	Time elapsed in seconds since the source has been known.
Expiry Time	Time left in seconds before the entry is removed.

Example

```
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, Config mode and all Config sub-modes

User Guidelines

The following information is displayed for the specified interface:

Field	Description
Interface	The interface number in unit/slot/port format.
MLD Global Admin Mode	This field displays the configured global administrative status of MLD.
MLD Interface Admin Mode	This field displays the configured interface administrative status of MLD.
MLD Operational Mode	The operational status of MLD on the interface.
MLD Version	This field indicates the version of MLD configured on the interface.
Query Interval	This field indicates the configured query interval for the interface.
Query Max Response Time	This field indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	This field displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.
Startup Query Interval	This value indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.

Last Member Query Interval	This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled:

Field	Description
Querier Status	This value indicates whether the interface is a MLD querier or non-querier on the subnet with which it is associated.
Querier Address	The IP address of the MLD querier on the subnet the interface with which it is associated.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.
Querier Expiry Time	Time left in seconds before the Querier loses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

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
Startup Query Count..... 2
Last Member Query Interval (milli-secs)..... 1111
Last Member Query Count..... 2

```

show ipv6 mld-proxy

Use the `show ipv6 mld-proxy` command to display a summary of the host interface status parameters.

Syntax

```
show ipv6 mld-proxy
```

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

Default Configuration

There is no default configuration for this command.

User Guidelines

The command displays the following parameters only when you enable MLD Proxy:

Field	Description
Interface Index	The interface number of the MLD Proxy interface.
Admin Mode	Indicates whether MLD Proxy is enabled or disabled. This is a configured value.

Operational Mode	Indicates whether MLD Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-Proxy interface sends unsolicited group membership reports.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

Example

```

console#show ipv6 mld-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-proxy groups

Use the `show ipv6 mld-proxy groups` command to display information about multicast groups that the MLD Proxy reported.

Syntax

`show ipv6 mld-proxy groups`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following parameters are displayed by this command:

Field	Description
Interface	The MLD Proxy interface.
Group Address	The IP address of the multicast group.
Last Reporter	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).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: <ul style="list-style-type: none">• Idle_Member—The interface has responded to the latest group membership query for this group.• Delay_Member—The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

Example

```
console#show ipv6 mld-proxy groups
Interface..... vlan 10
Group Address Last Reporter Up Time Member State Filter Mode Sources
-----
--
```

```

FF1E::1      FE80::100:2.3  00:01:40  DELAY_MEMBER  Exclude  2
FF1E::2      FE80::100:2.3  00:02:40  DELAY_MEMBER  Include  1
FF1E::3      FE80::100:2.3  00:01:40  DELAY_MEMBER  Exclude  0
FF1E::4      FE80::100:2.3  00:02:44  DELAY_MEMBER  Include  4

```

show ipv6 mld-proxy groups detail

Use the `show ipv6 mld-proxy groups detail` command to display information about multicast groups that MLD Proxy reported.

Syntax

```
show ipv6 mld-proxy groups detail
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following parameters are displayed by this command:

Field	Description
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	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).
Up Time (in secs)	The time elapsed in seconds since last created.

Member State	Possible values are: <ul style="list-style-type: none"> • Idle_Member—The interface has responded to the latest group membership query for this group. • Delay_Member—The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	The time left for a source to get deleted.

Example

```

console#show ipv6 igmp-proxy groups
Interface..... vlan 10

Group Address Last Reporter   Up Time   Member State   Filter Mode
Sources
-----
FF1E::1      FE80::100:2.3   244      DELAY_MEMBER   Exclude        2

Group Source List           Expiry Time
-----
2001::1              00:02:40
2001::2              -----

FF1E::2      FE80::100:2.3   243      DELAY_MEMBER   Include        1

Group Source List           Expiry Time
-----
3001::1              00:03:32
3002::2              00:03:32

FF1E::3      FE80::100:2.3   328      DELAY_MEMBER   Exclude        0
FF1E::4      FE80::100:2.3   255      DELAY_MEMBER   Include        4

Group Source List           Expiry Time
-----
4001::1              00:03:40

```

```
5002::2          00:03:40
4001::2          00:03:40
5002::2          00:03:40
```

show ipv6 mld-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-proxy interface
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

The following parameters are displayed only when MLD Proxy is enabled:

Parameter	Description
Interface	The MLD Proxy interface.

The column headings of the table associated with the interface are as follows:

Parameter	Description
Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

Example

```
console#show ipv6 mld-proxy interface
```

```
Interface..... vlan 10
```

```
Ver Query Rcvd Report Rcvd Report Sent Leave Rcvd  
Leave Sent
```

```
-----  
-----  
1      2          0          0          0          2  
2      3          0          4          -----  -----
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Field	Description
Valid MLD Packets Received	The number of valid MLD packets received by the router.

Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.
Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

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
```

show ipv6 neighbors

Use the `show ipv6 neighbors` command in Privileged EXEC mode to display information about the IPv6 neighbors.

Syntax

`show ipv6 neighbors`

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

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 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]

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
Static..... 1
OSPF Intra-area routes..... 110
OSPF Inter-area routes..... 110
OSPF External routes..... 110
```

show ipv6 route summary

Use the `show ipv6 route summary` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the routing table.

```
console#show ipv6 route summary
IPv6 Routing Table Summary - 0 entries
Connected Routes..... 0
```

```

Static Routes..... 0
OSPF Routes..... 0
Intra Area Routes..... 0
Inter Area Routes..... 0
External Type-1 Routes..... 0
External Type-2 Routes..... 0
Total routes..... 0
Number of Prefixes:

```

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** — Tunnel identifier. (Range: 0-7)
- **loopback** — Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode, Config mode and all Config sub-modes

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
```

```
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
```

```

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 in Privileged EXEC mode to display IPv6 VLAN routing interface addresses.

Syntax

```
show ipv6 vlan
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 in Privileged EXEC mode to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

Syntax

```
traceroute ipv6 {ip-address | hostname} [port]
```

- *ipv6-address* — Destination IPv6 address.

- *hostname* — Hostname to ping (contact). (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, `console(config)#traceroute "host name"`
- *port* — UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. (Range: 0–65535)

Default Configuration

33434 is the default port value.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example discovers the packet routes on a hop-by-hop basis.

```
console#traceroute ipv6 2020:1::1
```

```
Tracing route over a maximum of 20 hops
```

```
1 * N * N * N
```

Loopback Interface Commands

PowerConnect 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.

Support for the internal loopback address, if present, is limited to testing the IP stack.

Commands in this Chapter

This chapter 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.

```
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```


Multicast Commands

The PowerConnect 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 Chapter

This chapter explains the following commands:

<code>ip mcast boundary</code>	<code>ip pim dr-priority</code>	<code>ip pim spt-threshold</code>	<code>show ip mcast mroute static</code>
<code>ip mroute</code>	<code>ip pim hello-interval</code>	<code>show ip multicast</code>	<code>show ip pim bsr-router</code>
<code>ip multicast</code>	<code>ip pim join-prune-interval</code>	<code>show ip multicast</code>	<code>show ip pim interface</code>
<code>ip multicast ttl-threshold</code>	<code>ip pim register-rate-limit</code>	<code>show ip mcast boundary</code>	<code>show ip pim neighbor</code>
<code>ip pim</code>	<code>ip pim rp-address</code>	<code>show ip multicast interface</code>	<code>show ip pim rp hash</code>
<code>ip pim bsr-border</code>	<code>ip pim rp-candidate</code>	<code>show ip mcast mroute</code>	<code>show ip pim rp mapping</code>
<code>ip pim bsr-candidate</code>	<code>ip pim sparse</code>	<code>show ip mcast mroute group</code>	–
<code>ip pim dense</code>	<code>ip pim ssm</code>	<code>show ip mcast mroute source</code>	–

ip mcast boundary

Use the **ip mcast 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 mcast boundary *groupipaddr* *mask*

no ip mcast boundary *groupipaddr* *mask*

- *groupipaddr*— IP address of multicast group. Valid range is 239.0.0.0 to 239.255.255.255.
- *mask*— IP mask of multicast group.

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 adds an administrative scope multicast boundary.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip mcast boundary 239.5.5.5  
255.255.255.255
```

ip mroute

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

Usage Guidelines

There are no user guidelines for this command.

Example

```
console(config)#
```

```
console(config)#ip mroute 1.1.1.1 255.255.0.0  
192.168.20.1 34
```

ip multicast

Use the **ip multicast** command in Global Configuration mode to set the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message is displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Syntax

`ip multicast`

no ip multicast

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 IP multicast on the router.

```
console#configure
console(config)#ip multicast
console(config)#no ip multicast
```

ip multicast ttl-threshold

Use the `ip multicast ttl-threshold` command in Interface 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 pimdm** command in Interface (VLAN) Configuration mode to administratively configure PIM mode for IP multicast routing on a VLAN interface. 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, multicast, and IGMP be enabled.

Example

```
console(config)#ip routing
console(config)#ip igmp
console(config)#ip multicast
```

```
console(config)#interface vlan 10
console(if-vlan-10)#ip pim
```

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. Lower values are preferred.

Example

```
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 cbsrhashmasklength` and `ip pimsm cbsrpreference` commands.

Syntax

```
ip pim bsr-candidate vlan { vlan-id hash-mask-length bsr-priority [interval interval]}  
no ip pim bsr-candidate vlan { vlan-id}
```

Parameter Description

Parameter	Description
<i>vlan-id</i>	A valid VLAN identifier with multicast routing enabled.
<i>hash-mask-length</i>	Length of the BSR hash to be ANDed with the multicast group address. (Range 0–32 bits). Default 0.
<i>bsr-priority</i>	The advertised priority of the BSR candidate. Range 0-255. Default 0.
<i>interval</i>	(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

Use the `ip pim dense` 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 dense mode. This command replaces the `ip pimsm` command.

Syntax

```
ip pim dense
```

```
no ip pim dense
```

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.

Example

```
console(config)#ip pim dense
```

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. This command deprecates the **ip pimsm query-interval**, the **ip pimsm hello-interval** and the **ip pimdm hello-interval** commands.

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

```
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. This command deprecates the `ip pimsm message-interval` and `ip pimsm join-prune-interval` commands.

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 register-rate-limit

Use the `ip pim register-rate-limit` command in Global Configuration mode to set a limit on the maximum number of PIM register messages sent per second for each (S,G) entry. Use the `no` form of this command to return the limit to its default value (0). This command replaces the `ip pimsm spt-threshold` command.

Syntax

```
ip pim register-rate-limit 0-2000
```

```
no ip pim register-rate-limit
```

Parameter Description

Parameter	Description
register-rate-limit	The PIM register message limit in kilobytes per second. Range 0-2000.

Default Configuration

The default threshold is 0. This indicates that the register limit is infinite.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)#ip pim register-rate-limit 10
```

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}
```

Parameter Description

Parameter	Description
<i>rp-address</i>	The valid IPv4 address for the rendezvous point.
<i>group-address</i>	A valid multicast group address to be sourced from the rendezvous point.
<i>group-mask</i>	A mask indicating the range of multicast groups sourced from the RP
<i>override</i>	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

There are no user guidelines for this command.

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 pimsm rp-candidate** command.

Syntax

```
ip pim rp-candidate vlan { vlanid group-address group-mask [interval interval]}  
no ip pim rp-candidate vlan vlanid group-address group-mask}
```

Parameter Description

Parameter	Description
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.

Example

```
console(config)#ip pim rp-candidate vlan 10 239.1.0.0  
255.255.0.0 interval 30
```

ip pim sparse

Use the `ip pim sparse` 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 sparse mode. This command replaces the `ip pimsm` command.

Syntax

ip pim sparse

no ip pim sparse

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.

Example

```
console(config)#ip pim sparse
```

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*}

Parameter Description

Parameter	Description
default	Defines the SSM range access list to 232/8.
<i>group-address</i>	An IP multicast group address.
<i>group-mask</i>	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
```

ip pim spt-threshold

Use the `ip pim spt-threshold` command in Global Configuration mode to set the multicast traffic threshold rate for the last-hop router to switch to the shortest path on the router. Use the **no** form of this command to return the threshold to its default value (0).

Syntax

```
ip pim spt-threshold spt-threshold
```

```
no ip pim spt-threshold
```

Parameter Description

Parameter	Description
spt-threshold	The multicast traffic threshold rate in kilobytes per second. Range: 0–2000 Kbps).

Default Configuration

The default threshold is 0. This indicates that the multicast router should always switch to the multicast source tree.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pim spt-threshold 100
```

show ip multicast

Use the **show ip multicast** command in Privileged EXEC mode to display the system-wide multicast information.

Syntax

```
show ip multicast
```

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide multicast information.

```
console#show ip multicast
Admin Mode..... Enabled
Protocol State..... Non-Operational
Table Max Size..... 256
Protocol..... PIMDM
```

show ip mcast boundary

Use the `show ip mcast boundary` command in Privileged EXEC mode to display all the configured administrative scoped multicast boundaries.

Syntax

`show ip mcast boundary {vlan vlan-id | all}`

- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays all the configured administrative scoped multicast boundaries.

```
console#show ip mcast boundary all
```

```
MULTICAST BOUNDARY
```

```
Interface  Group  Ip Mask
```

```
-----  -
```

show ip multicast interface

Use the `show ip multicast interface` command in Privileged EXEC mode to display the multicast information for the specified interface.

Syntax

show ip multicast interface [type number]

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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
-----
```

show ip mcast mroute

Use the `show ip mcast mroute` command in Privileged EXEC mode to display a summary or all the details of the multicast table.

Syntax

show ip mcast mroute {detail | summary}

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary or all the details of the multicast table.

```
console#show ip mcast mroute summary
```

```
console#show ip mcast mroute detail
```

show ip mcast mroute group

Use the `show ip mcast mroute group` command in Privileged EXEC mode 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 mcast mroute group groupipaddr {detail | summary}
```

- *groupipaddr*— IP address of the multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 mcast mroute group 224.5.5.5 summary
```

```
console#show ip mcast mroute group 224.5.5.5 detail
```

show ip mcast mroute source

Use the `show ip mcast mroute source` command in Privileged EXEC mode 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 mcast 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays multicast configuration settings.

```
console#show ip mcast mroute source 10.1.1.1 summary
```

```
console#show ip mcast mroute source 10.1.1.1 224.5.5.5
```

show ip mcast mroute static

Use the `show ip mcast mroute static` command in Privileged EXEC mode 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 mcast mroute static [sourceipaddr]
```

- *sourceipaddr*— IP address of source.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 mcast mroute static
```

```

                                     MULTICAST STATIC ROUTES
Source IP           Source Mask   RPF Address
Preference
```


1.1.1.1 255.255.255.0 2.2.2.2 23

show ip pim bsr-router

The `show ip pim bsr-router` command displays information about a bootstrap router (BSR). This command deprecates the `show ip pimsm componenttable` and `show ip pimsm bsr` commands.

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, Config mode and all Config sub-modes

User Guidelines

The following information is displayed:

Field	Description
BSR address	IP address of the BSR.
BSR Priority	The configured BSR priority.
BSR Hash Mask Length	The configured hash mask length (32 bits maximum).
Next Bootstrap Message in	Time remaining (in hours, minutes, and seconds) until a BSR message is sent.
Next Candidate RP Advertisement	Time remaining (in hours, minutes, and seconds) until the next RP advertisement is sent.

Example

```
console#show ip pim bsr-router
```

```
BSR Address..... 192.168.10.1
BSR Priority..... 0
BSR Hash Mask Length..... 30
C-BSR Advertisement Interval (secs).....60
Next Bootstrap message (hh:mm:ss)..... NA
```

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. This command deprecates the `show ip pimsm interface stats`, `show ip pimsm interface` and `show ip pimdm interface` commands.

Syntax

```
show ip pim interface [vlan vlan-id]
```

- *vlan-id*— A valid VLAN ID for which multicast routing has been enabled.

Field Descriptions

Field	Description
Mode	Active PIM Protocol
Interface	Interface number
Hello Interval	Hello interval value
Join-prune Interval	Join-prune interval value
DR Priority	DR Priority configured on this interface

Field	Description
BSR Border	Whether or not this interface is configured as a BSR Border
Neighbor Count	Number of PIM Neighbors learnt on this interface
Designated-Router	IP address of the elected DR on the interface

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC and Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
(console) #show ip pim interface
```

```
InterfaceVLAN0010
  ModeSparse
  Hello Interval (secs)30
  Join Prune Interval (secs)60
  DR Priority1
  BSR BorderDisabled
  Neighbor Count1
  Designated Router192.168.10.1
```

```
InterfaceVLAN0001
  ModeSparse
```

```
Hello Interval (secs)30
Join Prune Interval (secs)60
DR Priority1
BSR BorderDisabled
Neighbor Count1
Designated Router192.168.10.1
```

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM
```

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Field Descriptions

Field	Description
Neighbor Addr	IP address of the PIM neighbor
Interface	Interface number
Uptime	Time since the neighbor is learned
Expiry Time	Time remaining for the neighbor to expire

Example

```
(console)#show ip pim neighbor vlan 10
                                     Up Time   Expiry Time
Neighbor Addr  Interface  hh:mm:ss  hh:mm:ss
-----
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)
-----
192.168.10.2   VLAN0001   00:02:55        00:01:15
192.168.20.2   VLAN0010   00:03:50        00:02:10
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Field	Description
RP Address	Address of the RP
Type	Origin from where this group mapping was learned.

Example

```
console#show ip pim rp hash 224.1.2.0
```

```
RP Address192.168.10.1
```

```
TypeStatic
```

If no RP Group mapping exists on the router, the following message is displayed:

```
No RP-Group mappings exist/learned on this router.ny  
interface.
```

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. This command deprecates the `show ip pimsm rp candidate`, `show ip pimsm staticrp`, `show ip pimsm rp mapping` commands.

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Field Descriptions

Field	Description
RP Address	Address of the RP
Group Address	Address of the multicast group.
Group Mask	Mask for the group address.
Origin	Origin from where this group mapping is learned.

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.

IPv6 Multicast Commands

This chapter explains the following commands:

<code>ipv6 pim (Global config)</code>	<code>ipv6 pim rp-candidate</code>
<code>ipv6 pim (VLAN Interface config)</code>	<code>ipv6 pim sparse (Global config)</code>
<code>ipv6 pim bsr-border</code>	<code>ipv6 pim spt-threshold</code>
<code>ipv6 pim bsr-candidate</code>	<code>ipv6 pim ssm</code>
<code>ipv6 pim dense</code>	<code>show ipv6 pim</code>
<code>ipv6 pim dr-priority</code>	<code>show ipv6 pim bsr</code>
<code>ipv6 pim hello-interval</code>	<code>ipv6 pim dense</code>
<code>ipv6 pim join-prune-interval</code>	<code>show ipv6 pim interface</code>
<code>ipv6 pim register-rate-limit</code>	<code>show ipv6 pim neighbor</code>
<code>ipv6 pim register-threshold</code>	<code>show ipv6 pim rphash</code>
<code>ipv6 pim rp-address</code>	<code>show ipv6 pim rp mapping</code>

ipv6 pim (Global config)

Use the `ipv6 pim` command to administratively enable PIMSM for IPv6 multicast routing. Use the `no` form of this command to disable PIMSM for IPv6.

Syntax

```
ipv6 pim
no ipv6 pim
```

Default Configuration

IPv6 PIMSM is disabled on the router by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pim
```

ipv6 pim (VLAN Interface config)

Use the `ipv6 pim` command in VLAN Interface configuration mode to administratively enable PIM-SM multicast routing mode on a particular IPv6 router interface. Use the `no` form of this command to disable PIM SM on an interface.

Syntax

```
ipv6 pim
```

```
no ipv6 pim
```

Default Configuration

PIM-SM 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
```

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

```
ipv6 pim bsr-candidate vlan vlan-id hash-mask-len [ priority ]
```

```
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).

Default Configuration

The router will not announce its candidacy by default.

The default hash mask length is 126 bits.

The default priority is 0.

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
```

ipv6 pim dense

Use the `ipv6 pim dense` command in Global configuration mode to administratively configure PIM dense mode for IPv6 multicast routing. Use the `no` form of this command to disable PIM dense mode.

Syntax

```
ipv6 pim dense
```

```
no ipv6 pim dense
```

Default Configuration

PIM is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

Only one of sparse or dense mode can be configured on a router.

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: 0–65535 seconds).

Default Configuration

The default hello interval is 30 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

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-rate-limit

Use the `ipv6 pim register-rate-limit` command to set a limit on the maximum number of PIM register messages sent per second for each (S,G) entry. Use the `no` form of this command to return the limit to its default value (0).

Syntax

```
ipv6 pim register-rate-limit register-rate-limit
```

```
no ipv6 pim register-rate-limit
```

Parameter Description

Parameter	Description
register-rate-limit	The PIM register message limit in kilobytes per second. Range 0–2000 Kbps.

Default Configuration

The default threshold is 0. This indicates that the register limit is infinite.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pim register-rate-limit 10
```

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*—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: 1–32)

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`

`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: 1–32)

Default Configuration

The router does not advertise itself as a PIM candidate rendezvous point by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pim rp-candidate vlan 6  
ff1e::/64
```

ipv6 pim sparse (Global config)

Use the `ipv6 pim sparse` command to administratively configure PIM sparse mode for multicast routing. Use the `no` form of this command to disable PIM sparse mode.

Syntax

`ipv6 pim sparse`

`no ipv6 pim sparse`

Default Configuration

IPv6 PIM is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

Only one of sparse or dense mode can be configured on a router.

Example

```
console(config)#ipv6 pim sparse
```

ipv6 pim spt-threshold

Use the `ipv6 pim spt-threshold` command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. Use the "no" form of this command to set the data threshold to the default.

Syntax

```
ipv6 pim spt-threshold threshold
```

```
no ipv6 pim spt-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 spt-threshold 1000
```

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 232/8.
- `group-address`—Group IP address supported by RP.
- `prefixlength`—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–32)

Default Configuration

There is no SSM range defined by default.

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pim
```

```
Admin Mode.....  
Enabled  
Data Threshold Rate (Kbps)..... 1000  
Register Threshold Rate (Kbps)..... 250
```

SSM RANGE TABLE

Group Address/Prefix Length

```
FF1E::/64
```

PIM-SM INTERFACE STATUS

Interface	Interface-Mode	Operational-Status
-----	-----	-----
vlan 3	Enabled	Operational
vlan 6	Enabled	Operational
vlan 9	Enabled	Operational

show ipv6 pim bsr

Use the `show ipv6 pim bsr` command to display the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Syntax

```
show ipv6 pim bsr
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pim bsr
```

```
BSR Address.....  
3001::1  
  
BSR Priority..... 23  
  
BSR Hash Mask Length..... 10  
  
Next bootstrap message (hh:mm:ss).....  
00:00:11  
  
Next Candidate RP advertisement (hh:mm:ss).....  
00:00:12
```

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

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command. Field descriptions are shown in the following table.

Field	Description
BSR Address	Address of the BSR
BSR Priority	Configured BSR priority
BSR Hash Mask Length	Configured hash mask length
Next Bootstrap Message	Remaining time until a BSR message is sent
Next Candidate RP Advertisement	Time remaining until the next RP advertisement is sent.

Example

```
console#show ipv6 pim bsr-router
```

```
BSR Address..... 2001:0db8:0:badc::1
  BSR Priority..... 0
  BSR Hash Mask Length..... 32
  C-BSR Advertisement Interval (secs)..... 60
  Next Bootstrap message (hh:mm:ss)..... 00:00:02
```

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 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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
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 [ all | 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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pim neighbor all
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 rphash

Use the `show ipv6 pim rphash` command to display which rendezvous point (RP) is being selected for a specified group.

Syntax

```
show ipv6 pim rphash 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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pim rphash ff1e::/64
```

RP Address	Type
3001::1	BSR

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*]

- *rp-address*—IP address of RP.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
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
```


OSPF Commands

OSPF is a link-state protocol. PowerConnect OSPF supports variable-length subnet masks. PowerConnect 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, PowerConnect routing supports OSPF version 2 in accordance with RFC 2328. The PowerConnect 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 PowerConnect 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. PowerConnect also supports OSPFv3 for use with IPv6 networks.

The PowerConnect 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

PowerConnect OSPF allows the administrator to change the preference for selecting intra, inter, and external routes according to the following rules:

- External route preferences apply to all ospf external routes like type1, type2, nssa-type1, nssa-type2 equally.
- Multiple route types may be configured with equal preference values.
- 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.

PowerConnect 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 StrataXGS® IV platforms, the ECMP hashing support is extended to 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

PowerConnect supports the flooding capability of opaque LSAs. PowerConnect 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 PowerConnect implementation of OSPFv2 supports graceful restart as specified in RFC 3623. Graceful restart works in concert with PowerConnect 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.

PowerConnect implements both the restarting router and helpful neighbor features described in RFC 3623.

Commands in this Chapter

This chapter explains the following commands:

area default-cost (Router OSPF)	capability opaque	ip ospf priority	show ip ospf asbr
area nssa (Router OSPF)	clear ip ospf	ip ospf retransmit-interval	show ip ospf database
area nssa default-info-originate (Router OSPF Config)	clear ip ospf stub-router	ip ospf transmit-delay	show ip ospf database database-summary
area nssa no- redistribute	compatible rfc1583	log adjacency-changes	show ip ospf interface
area nssa no-summary	default-information originate (Router OSPF Configuration)	max-metric router-lsa	show ip ospf interface brief
area nssa translator-role	default-metric	maximum-paths	show ip ospf interface stats

area nssa translator-stab-intv	distance ospf	network area	show ip ospf neighbor
area range (Router OSPF)	distribute-list out	nsf	show ip ospf range
area stub	enable	nsf helper	show ip ospf statistics
area stub no-summary	exit-overflow-interval	nsf helper strict-lsa-checking	show ip ospf stub table
area virtual-link	external-lsdb-limit	nsf restart-interval	show ip ospf traffic
area virtual-link authentication	ip ospf area	passive-interface default	show ip ospf virtual-link
area virtual-link dead-interval	ip ospf authentication	passive-interface	show ip ospf virtual-links brief
area virtual-link hello-interval	ip ospf cost	redistribute	show routing heap summary
area virtual-link retransmit-interval	ip ospf database-filter all out	router-id	timers pacing flood
area virtual-link transmit-delay	ip ospf dead-interval	router ospf	timers pacing lsa-group
auto-cost	ip ospf hello-interval	show ip ospf	timers spf
bandwidth	ip ospf mtu-ignore	show ip ospf abr	–
–	ip ospf network	show ip ospf area	–

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]
```

Parameter Description

Parameter	Description
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 : 1 A metric type of nssa-external 1 2 A metric type of nssa-external 2 (default)
role	The translator role where role is one of the following : <ul style="list-style-type: none">• 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.

```
console(config)#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 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 non-comparable (`nssa-external 2`). Use the `no` form of the command to return the metric value and type to the default value.

Syntax

```
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.

```
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 deposited 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}
```

Parameter Description

Parameter	Description
<i>area-id</i>	Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
<i>prefix netmask</i>	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 (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 (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 (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 (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 (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(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

This command has no user guidelines.

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 has no user guidelines.

Example

The following example prevents the Summary LSA from being advertised into the area 3 NSSA.

```
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]]

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]]

Parameter Description

Parameter	Description
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 acknowledgement 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

Parameter	Default
area-id	No area ID is predefined.
router-id	No router ID is predefined.
hello-interval seconds	10 seconds
retransmit-interval seconds	5 seconds
transmit-delay seconds	1 second
dead-interval seconds	40 seconds
authentication-key key	No key is predefined.
message-digest-key key-id md5 key	No key is predefined.

Command Mode

Router OSPF Configuration mode.

User Guidelines

Unauthenticated interfaces cannot be configured with an authentication key. Use the [area virtual-link authentication](#) command on page 1224 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:

```
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:

```
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.

```
console(config-router)#area 10 virtual-link
192.168.2.7 authentication

console(config-router)#area 10 virtual-link
192.168.2.7 authentication encrypt test123 1001010
```

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

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.

```
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 acknowledgement 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 ($\text{ref_bw} / \text{interface bandwidth}$), 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: 1–10000000).

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
```

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]]}]
```

- **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.

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

The following example shows the options for the **clear ip ospf** command.

```
console#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 reoriginate external LSAs
```

clear ip ospf stub-router

Use the **clear ip ospf stub-router** command in Privileged EXEC mode 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
```

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.

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

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]`

Syntax Description

Parameter	Description
<code>always</code>	Always advertise default routes.
<code>metric-value</code>	The metric (or preference) value of the default route. (Range: 1–16777214)
<code>type-value</code>	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(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}
```

Syntax Description

Parameter	Description
<code>intra-area dist1</code>	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).
<code>inter-area dist2</code>	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).
<code>external dist3</code>	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 {rip | static | connected}
```

```
no distribute-list name out {rip | static | connected}
```

Syntax Description

Parameter	Description
name	The name used to identify an existing ACL. The range is 1–31 characters.
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 reset the default administrative mode of OSPF in the router (active). 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

This command has no user guidelines.

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 its 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 (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.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
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.

```
console(config-if-vlan15)#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

```
ip ospf dead-interval seconds
```

no ip ospf dead-interval

- *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.

```
console(config-if-vlan15)#ip ospf dead-interval 30
```

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-vlan15)#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-vlan15)#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.

Usage 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.

```
console(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-vlan15)#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-vlan15)#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-vlan15)#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**]

Parameter Description

Parameter	Description
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]
```

Parameter Description

Parameter	Description
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(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

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 subnet.
- *area-id* — The ID of the area (Range: IP address or decimal from 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.

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 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 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

```
console (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

```
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

```
console (config-router) #passive-interface vlan 1
```

redistribute

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]

Parameter Description

Parameter	Description
protocol	rip - Specifies RIP as the source protocol. static - Specifies that the source is a static route. connected - Specifies that the source is a directly connected route.
static	Specifies that the source is a static route.
connected	Specifies that the source is a directly connected route.
metric-value	Specifies the metric to use when redistributing the route. (Range: 0–16777214)
type-value	Type 1 external route. Type 2 external route.
tag-value	Value attached to each external route, which might be used to communicate information between ASBRs. (Range: 0–4294967295)
subnets	Specifies whether to redistribute the routes to subnets.

Default Configuration

0 is the tag-value default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

```
console(config-router)#redistribute rip metric 90  
metric-type 1 tag 555 subnets
```

router-id

Use the **router-id** command in Router OSPF Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.

Syntax

```
router-id ip-address
```

- *ip-address* — IP address that uniquely identifies the router OSPF ID.

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 defines the router OSPF 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.

Syntax

```
router ospf
```

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

The command prompt changes when the **router ospf** command executes.

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
```

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, Config mode and all Config sub-modes

User Guidelines

Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

Field	Description
Router ID	A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether OSPF is administratively enabled or disabled.
RFC 1583 Compatibility	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.
External LSDB Limit	Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.
Spf Delay Time	The number of seconds to wait before running a routing table calculation after a topology change.
Spf Hold Time	The minimum number of seconds between routing table calculations.
Flood Pacing Interval	The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the timers pacing flood command.
LSA Refresh Group Pacing Time	The size of the LSA refresh group window, in seconds. This is the value configured with the timers pacing lsa-group command.
Opaque Capability	Shows whether router is capable of sending Opaque LSAs.

AutoCost Ref BW	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.
Default Passive Setting	When enabled, OSPF interfaces are passive by default.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.
Default Metric	Default metric for redistributed routes.
Stub Router Configuration	One of Always , Startup , or None .
Stub Router Startup Time	Configured value in seconds. This row is only listed if OSPF is configured to be a stub router at startup.
Summary LSA Metric Override	One of Enabled (<i>met</i>), Disabled , where <i>met</i> is the metric to be sent in summary LSAs when in stub router mode.
Default Route Advertise	When enabled, OSPF originates a type 5 LSA advertising a default route.
Always	When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.
Metric Type	Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.
Number of Active Areas	The number of OSPF areas to which the router is attached on interfaces that are up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	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 re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	One of Active or Active .

Stub Router Reason	One of Configured , Startup , or Resource Limitation . This row is only listed if stub router is active.
Stub Router Time Remaining	The remaining time until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode.
External LSDB Overflow	OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs received.
AS_OPAQUE LSA Checksum	Sum of the checksums of all AS Opaque LSAs in the link state database.
New LSAs Originated	Shows the number of link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.
LSA Count	The number of LSAs in the link state database.
Maximum Number of LSAs	The limit on the number of LSAs that the router can store in its link state database.
LSA High Water Mark	The maximum number of LSAs that have been in the link state database since OSPF began operation.
AS Scope LSA Flood List Length	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.
Retransmit List Entries	The current number of entries on all neighbors' retransmit lists.
Maximum Number of Retransmit Entries	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.
Retransmit Entries High Water Mark	The maximum number of retransmit list entries that have been on all neighbors' retransmit lists at one time.

NSF Support	Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.
NSF Restart Interval	The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.
NSF Restart Status	Whether the router is currently performing a graceful restart.
NSF Restart Age	The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.
NSF Restart Exit Reason	The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.
NSF Helper Support	Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.
NSF Helper Strict LSA Checking	As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.
Redistributing	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.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, or RIP.
Tag	Shows the decimal value attached to each external route.
Subnets	When this option is not configured, OSPF will only redistribute classful prefixes.
Distribute-List	Shows the access list used to filter redistributed routes.

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 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>)

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
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip ospf abr
```

Type	Router Id	Cost	Area ID	Next	
Hop	Next Hop				
					I
ntf					
-----	-----	-----	-----	-----	-

INTRA	3.3.3.3	1	0.0.0.1	10.1.23.3	v
lan11					
INTRA	4.4.4.4	10	0.0.0.1	10.1.24.4	v
lan12					

show ip ospf area

Use the `show ip ospf area` command in Privileged EXEC mode to display information about the identified OSPF area.

Syntax

```
show ip ospf area area-id
```

Field	Description
<i>area-id</i>	Identifies the OSPF area whose ranges are being displayed. (Range: 0–4294967295)
Flood List Length	The number of LSAs waiting to be flooded within the area.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ip ospf asbr
```

Type	Router Id	Cost	Area ID	Next Hop	Next Hop
INTRA	1.1.1.1	1	0.0.0.1	10.1.12.1	vlan1
0					
INTRA	4.4.4.4	10	0.0.0.1	10.1.24.4	vlan1
2					

show ip ospf database

Use the `show ip ospf database` command in Privileged EXEC mode 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 [area-id] database [{asbr-summary | external | network | nssa-external | router | summary}] [ls-id] [adv-router [ip-address] | self-originate]
```

- *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.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

Information is only displayed if OSPF is enabled.

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)

Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt
5.2.0.0	0.0.0.0	1360	80000006 3a1f	-----	-----
5.2.0.0	5.2.0.0	1360	80000009 a47e	-----	---E-
20.20.20.20	20.20.20.20	1165	8000000b 0f80	-E----	-----

Network Link States (Area 0.0.0.0)

Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt
2.2.2.2	20.20.20.20	1165	80000005 f86d	-E--O-	

Network Summary States (Area 0.0.0.0)

Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt
5.2.0.0	0.0.0.0	1360	80000007 242e	-----	

Summary ASBR States (Area 0.0.0.0)

Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt
---------	------------	-----	----------------	---------	---------

```
5.2.0.0          0.0.0.0          1361  80000006 183a  -----
```

Link Opaque States (Area 0.0.0.0)

```
Link Id          Adv Router        Age    Sequence Chksm  Options Rtr Opt
-----
5.2.0.0          0.0.0.0          1361  80000005 ef59  -----
```

Area Opaque States (Area 0.0.0.0)

```
Link Id          Adv Router        Age    Sequence Chksm  Options Rtr Opt
-----
5.2.0.0          0.0.0.0          1362  80000005 e166  -----
```

AS External States

```
Link Id          Adv Router        Age    Sequence Chksm  Options Rtr Opt
-----
6.0.0.0          5.2.0.0          1364  80000008 e35d
```

AS Opaque States

```
Link Id          Adv Router        Age    Sequence Chksm  Options Rtr Opt
-----
5.2.0.0          0.0.0.0          1364  80000005 d373
```


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

```
show ip ospf database database-summary
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Field	Description
Router	Shows Total number of router LSAs in the OSPF link state database.
Network	Shows Total number of network LSAs in the OSPF link state database.
Summary Net	Shows Total number of summary network LSAs in the database.
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.
-------	--

Example

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
Type-7 Ext.....	0
Opaque Link.....	0
Opaque Area.....	0
Type-5 Ext.....	0
Self-Originated Type-5 Ext.....	0
Opaque AS.....	0
Total.....	0

show ip ospf interface

Use the `show ip ospf interface` command in Privileged EXEC mode 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 [interface-type interface-number]`

Syntax Description

Parameter	Description
interface-type	Vlan or loopback
interface-number	Valid VLAN ID or loopback interface number (Range: 0-7).
Flood Blocking	Indicates if flood blocking is enabled or disabled.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

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 3.

```
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
Iftransit 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..... 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 in Privileged EXEC mode to display brief information for the IFO object or virtual interface tables.

Syntax

show ip ospf interface brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays brief information for the IFO object or virtual interface tables.

```
console#show ip ospf interface brief
```

```
Router Hello Dead Retrax Retrax LSAAck
```

```
Interface AdminMode Area
```

```
ID Priority Intval Intval Intval Delay Intval
```

```
-----
```

vlan1	Enable	0.0.0.10	1	10	40
5	1	1			
vlan2	Disable	0.0.0.0	1	10	40
5	1	1			
vlan3	Disable	0.0.0.0	1	10	40
5	1	1			
loopback2	Disable	0.0.0.0	1	10	40
5	1	1			

show ip ospf interface stats

Use the `show ip ospf interface stats` command in User EXEC mode 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

Privileged EXEC mode, Config mode and all Config sub-modes

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 vlan15
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 neighbor

Use the `show ip ospf neighbor` command in Privileged EXEC mode to display information about OSPF neighbors. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

```
show ip ospf neighbor [interface-type interface-number] [neighbor-id]
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following examples display information about OSPF neighbors on the specified Ethernet and IP interfaces.

```
console#show ip ospf neighbor 3.3.3.3
```

```
Interface..... 0/25
Neighbor IP Address..... 172.20.25.3
Interface Index..... 25
Area Id..... 0.0.0.0
Options..... 0x2
Router Priority..... 1
Dead timer due in (secs)..... 10
Up Time..... 4 days 3
hrs 33 mins 36 secs
State..... Full/PtP
Events..... 4
Retransmitted LSAs..... 32
Retransmission Queue Length..... 0
Restart Helper Status..... Not helping
Restart Helper Exit Reason..... Not attempted
```

Field Description

Field	Description
Interface	The name of the interface on which the adjacency is formed.
Neighbor IP Address	The IPv4 address on the neighbor's interface used to form the adjacency.
Interface Index	The SNMP interface index.
Area Id	The OSPF area in which the adjacency is formed.
Options	The options advertised by the neighbor.
Router Priority	The router priority advertised by the neighbor.

Field	Description
Dead timer	The number of seconds until the dead timer expires.
Up Time	How long this adjacency has been in FULL state.
State	The current state of the adjacency.
Events	Incremented for the following events: <ul style="list-style-type: none"> • A DD is received from the neighbor with an MTU mismatch. • The neighbor sent an ACK for an LSA not on the neighbor's retransmit list. • The state of the adjacency changed.
Retransmitted LSAs	The number of LSAs retransmitted to a given neighbor.
Retransmission Queue Length	The number of LSAs on the neighbor's retransmit queue waiting for the neighbor to acknowledge.
Restart Helper Status	One of two values: <ul style="list-style-type: none"> • 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. • Not Helping — This router is not a helpful neighbor at this time.

Field	Description
Restart Helper Exit Reason	<p>One of the following values:</p> <ul style="list-style-type: none"> • Restart Reason — When the router is in helpful neighbor mode, the output includes the restart reason the restarting router sent in its grace LSA. The Restart Reason is the value in the Graceful Restart Reason TLV in the grace LSA sent by the restarting router. Possible values for the Restart Reason are defined in RFC 3623 as follows: <ul style="list-style-type: none"> – Unknown (0) – Software restart (1) – Software reload/upgrade (2) – Switch to redundant control processor (3) – Unrecognized - a value not defined in RFC 3623 <p>When the switch sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the initiate failover command is invoked), and to Unknown on an unplanned warm restart.</p> • Remaining Grace Time — The number of seconds remaining in the current graceful restart interval. This row is only included if the router is currently acting as a restart helper for the neighbor. • Restart Exit Reason — One of the following: <ul style="list-style-type: none"> – None — graceful restart has not been attempted – In Progress — restart is in progress – Completed — the previous graceful restart completed successfully – Timed Out — the previous graceful restart timed out – Topology Changed — The previous graceful restart terminated prematurely because of a topology change. A helpful neighbor declares a topology change when it forwards a changed LSA to the restarting router. An LSA is considered changed if its contents are changed, not if it is simply a periodic refresh.

show ip ospf range

Use the `show ip ospf range` command in Privileged EXEC mode to display information about the area ranges for the specified area-id.

Syntax

`show ip ospf range area-id`

Field Descriptions

Field	Description
<i>area-id</i>	Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0–4294967295)
Prefix	The summary prefix.
Subnet Mask	The subnetwork mask of the summary prefix.
Type	S (Summary Link) or E (External Link)
Action	Advertise or Suppress
Cost	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 .
Active	Whether the range is currently active (Y) or not (N).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Field Descriptions

Field	Description
Delta T	The time since the routing table was computed, in hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time to compute routes, in milliseconds. The total may exceed the sum of the Intra, Summ, and Ext times.

RIB Update	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.
Reason	The event or events that triggered the SPF. Reasons may include the following: <ul style="list-style-type: none"> • 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
```

Delta T Reason	Intra	Summ	Ext	SPF Total	RIB Update
00:05:33	0	0	0	0	0 R
00:05:30	0	0	0	0	0 R
00:05:19 N, SN	0	0	0	0	0
00:05:15 R, N, SN	0	10	0	10	0
00:05:11	0	0	0	0	0 R
00:04:50 R, N	0	60	0	60	460
00:04:46 R, N	0	90	0	100	60
00:03:42	0	70	10	90	160 R
00:03:39 X	0	70	40	120	240
00:03:36 X	0	60	60	130	160

00:01:28	0	60	50	130	240
X					
00:01:25	0	30	50	110	310
SN					
00:01:22	0	0	40	50	260
SN					
00:01:19	0	0	20	20	190 X
00:01:16	0	0	0	0	110
R, X					

show ip ospf stub table

Use the **show ip ospf stub table** command in Privileged EXEC mode 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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
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 in Privileged EXEC mode 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`

Parameter Description

Parameter	Description
OSPFv2 Packet Statistics	The number of packets of each type sent and received since OSPF counters were last cleared.
LSAs Retransmitted	The number of LSAs retransmitted by this router since OSPF counters were last cleared.
LS Update Max Receive Rate	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.
LS Update Max Send Rate	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.
Number of LSAs Received	The number of LSAs of each type received since OSPF counters were last cleared.

Parameter	Description
OSPFv2 Queue Statistics	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.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode

User Guidelines

The `clear ip ospf counters` command does not clear the message queue high water marks.

Example

```
console# show ip ospf traffic
```

```
Time Since Counters Cleared: 4000 seconds
```

```
OSPFv2 Packet Statistics
```

```

      Hello   Database Desc   LS Request   LS Update   LS
ACK   Total
Recd:    500             10           20           50
20     600
Sent:    400             8            16           40
16     480

```

```
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

	Current	Max	Drops	Limit
Hello	0	10	0	500
ACK	2	12	0	1680
Data	24	47	0	500
Event	1	8	0	1000

show ip ospf virtual-link

Use the `show ip ospf virtual-link` command in Privileged EXEC mode to display the OSPF Virtual Interface information for a specific area and neighbor or for all.

Syntax

```
show ip ospf virtual-link [area-id neighbor-id]
```

- *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, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for area 10 and its neighbor.

```
console#show ip ospf virtual-link 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 in Privileged EXEC mode to display the OSPF Virtual Interface information for all areas in the system in table format. **Syntax**

```
show ip ospf virtual-link brief
```

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information in the system.

```
console#show ipv6 ospf virtual-link brief
                                Hello    Dead      Retransmit  T
ransit
Area
ID Neighbor      Interval Interval Interval      Delay
-----
-----
```

0.0.0.2 5.5.5.5

10

40

5

1

show routing heap summary

Use the `show routing heap summary` command in Privileged EXEC mode to display a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Syntax

`show routing heap summary`

Parameter Description

The command displays the following information.

Parameter	Description
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following shows example CLI display output for the command.

```
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%)
```

timers pacing flood

Use the **timers pacing flood** command in router OSPF Global Configuration mode 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

Parameter Description

Parameter	Description
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 in router OSPF Global Configuration mode to tune how OSPF groups LSAs for periodic refresh.

Syntax

`timers pacing lsa-group seconds`

Parameter Description

Parameter	Description
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

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 LS Update packets. Minimizing the number of Update 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.

timers spf

Use the **timers spf** command in Router OSPF Configuration mode 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

This chapter explains the following commands:

area default-cost (Router OSPFv3)	area virtual-link transmit-delay	ipv6 ospf priority	show ipv6 ospf abr
area nssa (Router OSPFv3)	default-information originate (Router OSPFv3 Configuration)	ipv6 ospf retransmit-interval	show ipv6 ospf area
area nssa default-info-originate (Router OSPFv3 Config)	default-metric	ipv6 ospf transmit-delay	show ipv6 ospf asbr
area nssa no- redistribute	distance ospf	ipv6 router ospf	show ipv6 ospf database
area nssa no-summary	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)	ipv6 ospf	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
area virtual-link dead-interval	ipv6 ospf hello-interval	redistribute	show ipv6 ospf stub table

area virtual-link hello-interval	ipv6 ospf mtu- ignore	router-id	show ipv6 ospf virtual- links
area virtual-link retransmit-interval	ipv6 ospf network	show ipv6 ospf	show ipv6 ospf virtual- link brief

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]
```

Parameter Description

Parameter	Description
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 : 1 A metric type of nssa-external 1 (comparable) 2 A metric type of nssa-external 2 (non-comparable)
role	The translator role where role is one of the following : <ul style="list-style-type: none">• 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(config)#ipv6 router ospf
console(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}
```

Parameter Description

Parameter	Description
<i>areaid</i>	Valid OSPFv3 area identifier.
<i>ipv6-prefix/prefix-length</i>	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(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.

Parameter Description

Parameter	Description
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(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 to 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.
- **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 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]
```

Parameter	Description
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 acknowledgement 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

Parameter	Default
area-id	No area ID is predefined.
router-id	No router ID is predefined.
hello-interval seconds	10 seconds
retransmit-interval seconds	5 seconds
transmit-delay seconds	1 second
dead-interval seconds	40 seconds

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.

```
console(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.

```
console(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

`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.

```
console(config)#ipv6 router ospf
```

```
console(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]
```

Syntax Description

Parameter	Description
always	Always advertise default routes.

Parameter	Description
metric-value	The metric (or preference) value of the default route. (Range: 1–16777214)
type-value	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
console(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.

```
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.

```
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(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

`ipv6 ospf retransmit-interval seconds`

`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(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

`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.

```
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 enter Router OSPFv3 Configuration mode.

Syntax

```
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

Use the **redistribute** command in Router OSPFv3 Configuration mode to configure the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

```
redistribute {static | connected} [metric metric] [metric-type {1 | 2}] [tag tag]
```

```
no redistribute {static | connected} [metric] [metric-type] [tag]
```

- *metric* — Metric value used for default routes. (Range: 0-16777214)
- *tag* — Tag. (Range: 0-4294967295)

Default Configuration

2 is the default value for **metric-type**, 0 for *tag*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

```
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

Field	Description
Router ID	A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether OSPF is administratively enabled or disabled.
External LSDB Limit	Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.
AutoCost Ref BW	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.
Default Passive Setting	When enabled, OSPF interfaces are passive by default.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.
Default Metric	Default metric for redistributed routes.
Default Route Advertise	When enabled, OSPF originates a type 5 LSA advertising a default route.

Always	When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.
Metric Type	Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.
Number of Active Areas	The number of OSPF areas to which the router is attached on interfaces that are up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	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 re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router	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 re-enable OSPF globally.
External LSDB Overflow	OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	Shows the number of link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.

LSA Count	The number of LSAs in the link state database.
Maximum Number of LSAs	The limit on the number of LSAs that the router can store in its link state database.
LSA High Water Mark	The maximum number of LSAs that have been in the link state database since OSPF began operation.
Retransmit List Entries	The current number of entries on all neighbors' retransmit lists.
Maximum Number of Retransmit Entries	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.
Retransmit Entries High Water Mark	The maximum number of retransmit list entries that have been on all neighbors' retransmit lists at one time.
NSF Support	Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.
NSF Restart Interval	The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.
NSF Restart Status	Whether the router is currently performing a graceful restart.
NSF Restart Age	The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.
NSF Restart Exit Reason	The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.
NSF Helper Support	Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.
NSF Helper Strict LSA Checking	As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.
Redistributing	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.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, or RIP.

Tag	Shows the decimal value attached to each external route.
Subnets	When this option is not configured, OSPF will only redistribute classful prefixes.
Distribute-List	Shows the access list used to filter redistributed routes.

Example

The following example enables OSPF traps.

```
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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf abr
```

Type Hop	Router Id	Cost	Area ID	Next Hop
	Intf			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
INTRA 3CB3	3.3.3.3 vlan11	10	0.0.0.1	FE80::211:88FF:FE2A: 3CB3
INTRA 8E1	4.4.4.4 vlan12	10	0.0.0.1	FE80::210:18FF:FE82: 8E1

show ipv6 ospf area

Use the `show ipv6 ospf area` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays information about area 1.

```
console#show ipv6 ospf area 1
AreaID..... 0.0.0.1
```

```

External Routing..... Import External LSAs
Spf Runs..... 0
Area Border Router Count..... 0
Area LSA Count..... 0
Area LSA Checksum..... 0
Stub Mode..... Disable
Import Summary LSAs..... Enable

```

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf asbr
```

Type	Router Id	Cost	Area ID	Next Hop	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, Config mode and all Config sub-modes

show ipv6 ospf database

Use the `show ipv6 ospf database` command in Privileged EXEC mode to display information about the link state database when OSPFv3 is enabled. 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.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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)

Adv Router      Link
Id              Age   Sequence Csum Options Rtr Opt
-----
1.1.1.1         0   4         80000034 54BD V
6E--R- ----B

2.2.2.2         0   2         80000044 95A5 V
6E--R- ----B

```

Network Link States (Area 0.0.0.0)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
2.2.2.2 6E--R-			636	636	80000001	8B0D V

Inter Network States (Area 0.0.0.0)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
1.1.1.1			1	323	80000001	3970
2.2.2.2			1	322	80000001	1B8A
1.1.1.1			2	293	80000001	3529
2.2.2.2			2	375	80000001	FC5E

Link States (Area 0.0.0.0)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
1.1.1.1 E--R-			634	700	80000008	2D89 V6
2.2.2.2 E--R-			634	689	8000000A	6F82 V6
2.2.2.2 E--R-			635	590	80000001	7782 V6

Intra Prefix States (Area 0.0.0.0)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
1.1.1.1			0	1	8000003C	9F31
2.2.2.2			0	2	8000004D	9126

Router Link States (Area 0.0.0.1)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
1.1.1.1 6E--R- --V-B			0	1	8000002E	35AD V
2.2.2.2 6E--R- ----B			0	0	8000004A	D2F3 V

Network Link States (Area 0.0.0.1)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr	Opt
1.1.1.1 6E--R-			634	621	80000001	B9E2 V

Inter Network States (Area 0.0.0.1)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr Opt
1.1.1.1			16	4	80000001 CA7C
2.2.2.2			18	3	80000001 B28D

Link States (Area 0.0.0.1)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr Opt
1.1.1.1 6E--R-			634	441	80000003 B877 V
2.2.2.2 6E--R-			634	433	80000003 FE6E V

Intra Prefix States (Area 0.0.0.1)

Adv Router Id	Age	Link Sequence	Csum	Options	Rtr Opt
1.1.1.1			0	6	8000003A 37C4
2.2.2.2			0	1	8000004F 439A
1.1.1.1			10634	434	80000002 440A

show ipv6 ospf database database-summary

Use the `show ipv6 ospf database database-summary` command in Privileged EXEC mode 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`

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

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 in Privileged EXEC mode to display the information for the IFO object or virtual interface tables.

Syntax

```
show ipv6 ospf interface [interface-type interface-number]
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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..... Err
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays brief ospf interface information.

```
console#show ipv6 ospf interface brief
```

Interface	Admin Mode	Area ID	Router Prior.	Cost	Hello Int. Val.	Dead Int. Val.	Retrax Int. Val.	Retrax Delay	LSA Ack Intval

show ipv6 ospf interface stats

Use the `show ipv6 ospf interface stats` command in User EXEC mode 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, Config mode and all Config sub-modes

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
  Packet Type                Sent          Received
-----
```

Packet Type	Sent	Received
Hello	295	219
Database Description	10	14
LS Request	4	4
LS Update	521	398
LS Acknowledgement	209	282

show ipv6 ospf interface vlan

Use the `show ipv6 ospf interface vlan` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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

```

show ipv6 ospf neighbor

Use the **show ipv6 ospf neighbor** command in Privileged EXEC mode to display information about OSPF neighbors. If a neighbor IP address is not specified, the output displays summary information in a table. If an interface or tunnel is specified, only the information for that interface or tunnel displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

`show ipv6 ospf neighbor [interface-type interface-number] [neighbor-id]`

Syntax Description

Parameter	Description
interface-type	Interface type, vlan or tunnel.
interface-number	A valid interface number, a valid VLAN ID or tunnel identifier. (Range is 0-7).
neighbor-id	Valid IP address of the neighbor about which information is displayed.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

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                                Ti
me
-----
```

```
console#show ipv6 ospf neighbor interface tunnel 1
```

```

IP Address..... Err
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

```

                                Hello      Dead      Retrans
mit Transit
Area
ID      Neighbor      Interval  Interval  Interval  D
elay
-----
-----
-----

```


Router Discovery Protocol Commands

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 Chapter

This chapter explains the following commands:

<code>ip irdp</code>	<code>ip irdp minadvertinterval</code>
<code>ip irdp address</code>	<code>ip irdp multicast</code>
<code>ip irdp holdtime</code>	<code>ip irdp preference</code>
<code>ip irdp maxadvertinterval</code>	<code>show ip irdp</code>

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
```

Syntax Description

Parameter	Description
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.

```
console (config) #interface vlan 15
console (config-if-vlan15) #ip irdp
```

ip irdp address

Use the **ip irdp address** command in Interface Configuration mode to configure the address that the interface uses to send the router discovery advertisements. Use the no form of the command to return the address to the default.

Syntax

ip irdp address *ip-address*

no ip irdp address

- *ip-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

IP address 224.0.0.1 is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines. This command is deprecated in favor of the **ip irdp multicast** command. If you issue this command, the configuration will show the **ip irdp multicast** command instead.

Example

The following example sets the limited broadcast address as the IP address for router discovery advertisements.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp address
255.255.255.255
```

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.

```
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

```
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.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp maxadvertinterval
600
```

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 15804 Router Discovery
Protocol Commands www.d e l l . c o m | s u p p o r t .
d e l l . c o m console(config-if-vlan15)#no 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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows router discovery information for VLAN 15.

```
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

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.

PowerConnect routing supports RIPv2 as specified in RFC 2453.

Commands in this Chapter

This chapter explains the following commands:

auto-summary	hostroutesaccept	router rip
default-information originate (Router RIP Configuration)	ip rip	show ip rip
default-metric	ip rip authentication	show ip rip interface
distance rip	ip rip receive version	show ip rip interface brief
distribute-list out	ip rip send version	split-horizon
enable	redistribute	—

auto-summary

Use the **auto-summary** command in Router RIP Configuration mode to enable the RIP auto-summarization mode. Use the no form of the command to disable auto-summarization 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 {ospf | static | connected}

no distribute-list *accesslistname* **out** {**ospf** | **static** | **connected**}

- *accesslistname* — The name used to identify the existing ACL. The range is 1-31 characters.
- **ospf** — Apply the specific 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

This command has no user guidelines.

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 sent 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

The **redistribute** command configures RIP protocol to redistribute routes from the specified source protocol/routers. 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
```

```
redistribute {static | connected} [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.

- `connected` — Redistributes directly-connected routes.

Default Configuration

`metric integer` — not configured

`match` — internal

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

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

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enters Router RIP mode.

```
console(config)#router rip
console(config-router)#
```

show ip rip

Use the `show ip rip` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays information relevant to the RIP router.

```
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

Link	Send	Receive	RIP	
Interface	IP			
Address	Version	Version	Mode	State
-----	-----	-----	-----	-----
vlan1	0.0.0.0	RIP-		
2	Both	Disable	Down	
vlan2	0.0.0.0	RIP-		
2	Both	Disable	Down	

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

PowerConnect 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, PowerConnect 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. PowerConnect 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 Chapter

This chapter explains the following commands:

interface tunnel	tunnel mode ipv6ip
show interfaces tunnel	tunnel source
tunnel destination	—

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
```

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.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel destination
10.1.1.1
```

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-tunnel1)#tunnel mode ipv6ip
console(config-if-tunnel1)#tunnel mode ipv6ip 6to4
```

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
```

Syntax Description

Parameter	Description
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.

```
console(config)#interface tunnel 1
```

```
console(config-if-tunnel1)#tunnel source vlan 11
```


Virtual Router Redundancy Protocol Commands

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 request 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.

PowerConnect 4.0 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 Chapter

This chapter explains the following commands:

Virtual Router Redundancy Protocol Commands

ip vrrp	vrrp timers advertise
vrrp accept-mode	vrrp timers learn
vrrp authentication	vrrp track interface
vrrp description	vrrp track ip route
vrrp ip	show vrrp
vrrp mode	show vrrp interface
vrrp preempt	show vrrp interface brief
vrrp priority	show vrrp interface stats

Pingable VRRP Commands

ip vrrp accept-mode	show ip vrrp interface
-------------------------------------	--

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 vid accept-mode
```

```
no vrrp vid accept-mode
```

- `vrvid` — 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.

vrrip authentication

Use the `vrrip 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

```
vrrip group authentication {none | simple key}
```

```
no vrrip group authentication
```

Syntax Description

Parameter	Description
<code>group</code>	The virtual router identifier. (Range: 1-255)
<code>none</code>	Indicates authentication type is none.
<code>simple</code>	Authentication type is a simple text password.
<code>key</code>	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(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
```

Syntax Description

Parameter	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. Descriptions containing spaces must be wrapped with quotes.

Example

The following example creates virtual router group 5 on VLAN 15 and configures its description.

```
console(config)#interface vlan 15
console(config-if-vlan15)#vrrp 5
console(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
```

Syntax Description

Parameter	Description
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)#ip routing
console(config)#ip vrrp
console(config)#vlan database
console(config-vlan)#vlan 15
console(config-vlan)#vlan routing 15
console(config-vlan)#exit
console(config)#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 192.168.5.20
console(config-if-vlan15)#vrrp 20 mode
```


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

Syntax Description

Parameter	Description
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, just the interface to be tracked without giving the priority, which is optional, then the default priority will be set.

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
```

Syntax Description

Parameter	Description
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

```
vrrp group track ip route ip-address/prefix-length [ decrement priority ]  
no vrrp group track ip route ip-address/prefix-length
```

Parameter Description

Parameter	Description
<i>group</i>	The virtual router identifier. (Range: 1–255).
<i>ip-address/prefix-length</i>	Specifies the route to be tracked.
<i>priority</i>	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]
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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
-----
Vl 1         2      60 0.0.0.0      Disable  Initialize
Vl 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}]
```

Syntax Description

Parameter	Description
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, Config mode and all Config sub-modes

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 7
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
```

show vrrp interface brief

Use the `show vrrp interface brief` command in Privileged EXEC mode to display information about each virtual router configured on the switch. It displays information about each virtual router.

Syntax

```
show vrrp interface brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

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

show vrrp interface stats

Use the `show vrrp interface stats` command in User EXEC mode to display the statistical information about each virtual router configured on the switch.

Syntax

```
show vrrp interface stats vlan vlan-id vr-id
```

- *vlan-id*— Valid VLAN ID.
- *vr-id*— The virtual router identifier. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays all statistical information about the VLAN 15 virtual router.

```
console#show vrrp interface stats vlan 15 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
```

Pingable VRRP Commands

ip vrrp accept-mode

Use the `ip 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. Use the **no** form of the command to disable responding to ping packets.

Syntax

```
ip vrrp vid 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

This command has no user guidelines.

show ip vrrp interface

Use the `show ip vrrp interface` command in User EXEC or Privileged EXEC mode to display the configured value for Accept Mode.

Syntax

show ip vrrp interface *interface-id* *vrid*

Syntax Description

Parameter	Description
interface-id	Any valid routing interface. See Interface Naming Conventions for interface representation.
vrid	The virtual router identifier. (Range: 1-255)

Default Configuration

The command has no default configuration.

Command Mode

User EXEC, Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays all configuration information about the VLAN 15 virtual router.

```
console#show ip vrrp interface vlan2 1
Primary IP Address..... 10.10.10.1
VMAC Address..... 00:00:5E:00:01:01
Authentication Type..... None
Priority..... 100
Configured Priority..... 100
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Disable
Accept Mode..... Enable
State..... Initialized
```

```
Track Interface State Decrement Priority
```

```
-----
```

```
No interfaces are tracked for this vrid and interface
combination.
```

```
Track Route(pfx/len) Reachable Decrement Priority
```

```
-----
```

```
No routes are tracked for this vrid and interface
combination.
```


Utility Commands

This section of the document contains the following Utility command topics:

Auto-Install Commands	Line Commands	SDM Templates Commands	Telnet Server Commands
Captive Portal Commands	Management ACL Commands	Serviceability Tracing Packet Commands	Terminal Length Commands
CLI Macro Commands	Mode Commands	Sflow Commands	Time Ranges Commands
Clock Commands	Password Management Commands	SNMP Commands	–
Command Line Configuration Scripting Commands	PHY Diagnostics Commands	SSH Commands	User Interface Commands
Configuration and Image File Commands	–	Syslog Commands	Web Server Commands
Denial of Service Commands	RMON Commands	System Management Commands	–

Auto-Install Commands

Auto-Install provides automatic update of the image and configuration of PowerConnect devices on boot up from a TFTP server as controlled by received DHCP options. It plays a critical role in the PowerConnect 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 PowerConnect 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 PowerConnect 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 Chapter

This chapter explains the following commands:

<code>boot auto-copy-sw</code>	<code>boot auto-copy-sw allow-downgrade</code>
<code>boot auto-copy-sw allow-downgrade</code>	<code>boot host autoreboot</code>
<code>boot host autoreboot</code>	<code>boot host autosave</code>
<code>boot host autosave</code>	<code>boot host dhcp</code>
<code>boot host dhcp</code>	<code>boot host retrycount</code>
<code>boot host retrycount</code>	<code>show auto-copy-sw</code>
<code>boot auto-copy-sw</code>	<code>show boot</code>

boot auto-copy-sw

Use the `boot auto-copy-sw` command in Privileged EXEC mode to enable or disable Stack Firmware Synchronization.

Use the `no` form of the command to disable Stack Firmware Synchronization.

Syntax

```
boot auto-copy-sw
```

```
no boot auto-copy-sw
```

Parameter Description

This command does not require a parameter description.

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 in Privileged EXEC mode 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
```

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is **Enable**.

Command Mode

Global Configuration

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 downgrade the firmware.

boot host autoreboot

Use the **boot host autoreboot** command in Global Configuration mode to enable rebooting the device (no administrative intervention) when the auto-image is successfully downloaded. Use the **no** form of this command to disable rebooting the device (no administrative intervention) when the auto-image is successfully downloaded.

Syntax

boot host autoreboot

no boot host autoreboot

Parameter Description

This command does not require a parameter description.

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-image download.

Example

```
console#  
console#configure  
console(config)#boot host autoreboot  
console(config)#no boot host autoreboot
```


boot host autosave

Use the **boot host autosave** 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 autosave
```

```
no boot host autosave
```

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines

Example

```
console#
```

```
console#configure
```

```
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`

Parameter Description

This command does not require a parameter description.

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 retrycount

The **boot host retrycount** 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 retrycount count`

`no boot host retrycount`

- *count* —The number of attempts to download a configuration (Range: 1–6).

Default Configuration

The default number of configuration download attempts is three.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines

Example

```
console#  
console#configure  
console(config)#boot host retrycount 5  
console(config)#no boot host retrycount
```

show auto-copy-sw

Use the `show auto-copy-sw` command in Privileged EXEC mode to display Stack Firmware Synchronization configuration status.

Syntax

`show auto-copy-sw`

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The `show switch` command also displays the switch firmware synchronization status.

Example

```
console#show auto-copy-sw
```

```
Stack Firmware Synchronization
```

```
Synchronization:           Enabled
SNMP Trap status:         Enabled
Allow Downgrade:         Enabled
```

show boot

Use the `show boot` command in Privileged EXEC mode to display the auto install configuration and the status.

Syntax

```
show boot
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show boot
```

```
AutoInstall Mode..... Started
```

```
AutoSave Mode..... Enabled
```

```
AutoReboot Mode..... Enabled
```

```
AutoInstall Retry Count..... 3
```

```
AutoInstall State..... Waiting for boot options
```


Captive Portal Commands

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 Chapter

This chapter explains the following commands:

Captive Portal Global Commands

authentication timeout	https port
captive-portal	show captive-portal
enable	show captive-portal status
http port	—

Captive Portal Configuration Commands

block	name (Captive Portal)
configuration	protocol
enable	redirect
group	redirect-url

interface	session-timeout
locale	verification

Captive Portal Client Connection Commands

captive-portal client deauthenticate	show captive-portal interface client status
show captive-portal client status	show captive-portal interface configuration status
show captive-portal configuration client status	—

Captive Portal Local User Commands

clear captive-portal users	user-logout
no user	user name
show captive-portal user	user password
user group	user session-timeout

Captive Portal Status Commands

show captive-portal configuration	show captive-portal configuration locales
show captive-portal configuration interface	show captive-portal configuration status

Captive Portal User Group Commands

user group	user group name
user group moveusers	—

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

```
console(config-CP)#authentication timeout 600
console(config-CP)#no authentication timeout
```

captive-portal

Use the **captive-portal** command to enter the captive portal configuration mode.

Syntax

`captive-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 monitor. 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 to monitor (Range: 1–65535).

Default Configuration

Captive portal only monitors port 80 by default.

Command Mode

Captive Portal Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#http port 81
```

```
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 from monitoring.

Syntax

```
https port port-num
```

no https port

- *port-num*—The port number to monitor (Range: 1–65535).

Default Configuration

Captive portal only monitors port 443 by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

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, Config mode and all Config sub-modes

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
Captive Portal 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, Config mode and all Config sub-modes

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
Authenticated 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
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 (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

```
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(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

```
console(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 Config mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#interface 1/0/2
```

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: Only locale 1 is supported)

Default Configuration

Locale 1 is configured by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

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 protocols mode is https.

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

There are no user guidelines for this command.

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

There are no user guidelines for 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, Config mode and all Config sub-modes

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..... 1/0/1
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, Config mode and all Config sub-modes

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	1/0/1
		0002.BC00.1291	10.254.96.48	1/0/2
2	cp2	0002.BC00.1292	10.254.96.49	1/0/3
3	cp3	0002.BC00.1293	10.254.96.50	1/0/4

```
console#show captive-portal configuration 1 client status
```

```
CP ID..... 1
CP Name..... cp1
Client
MAC Address      Client
                  IP Address  Interface  Interface Description
-----
0002.BC00.1290  10.254.96.47  1/0/1     Unit: 1 Slot: 0 Port: 1 Gigabit
0002.BC00.1291  10.254.96.48  1/0/2     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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal interface client status
```

Intf	Intf Description	Client	
		MAC Address	IP Address
1/0/1	Unit: 1 Slot: 0 Port: 1 Gigabit	0002.BC00.1290	10.254.96.47
		0002.BC00.1291	10.254.96.48
1/0/2	Unit: 1 Slot: 0 Port: 2 Gigabit	0002.BC00.1292	10.254.96.49
1/0/3	Unit: 1 Slot: 0 Port: 3 Gigabit	0002.BC00.1293	10.254.96.50

```
console#show captive-portal interface 1/0/1 client status
```

```
Interface..... 1/0/1
```

```
Interface Description..... Unit: 1 Slot: 0 Port: 1 Gigabit
```

Client MAC Address	Client 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, Config mode and all Config sub-modes

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      1/0/1         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
-----
1/0/1         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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal user
```

```
Session
```

```
User ID      User Name      Timeout      Group ID
  Group Name
```

```

-----
-----
1          user123                14400      1
Default
2          user234                0          1
Default

                                2
group2

```

```

console#show captive-portal user 1
User ID..... 1
User Name.....
user123
Password Configured..... Yes
Session Timeout..... 0

```

```

Group ID          Group Name
-----
1          Default
2          group2

```

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

Parameter Description

This command does not require a parameter description.

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 (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 (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, Config mode and all Config sub-modes

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration 1 interface
CP ID..... 1
CP Name..... cp1
```

Interface	Interface Description	Operational Status	Block
1/0/1	Unit: 1 Slot: 0 Port: 1 Gigabit - Level	Disabled	Blocked

```
console#show captive-portal configuration 1 interface 1/0/1
CP ID..... 1
CP Name..... cp1
Interface..... 1/0/1
Interface Description..... Unit: 1 Slot: 0 Port: 1
Gigab...
Operational Status..... Disabled
Disable Reason..... Interface Not Attached
Block Status..... Not Blocked
Authenticated Users..... 0
```

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration 1 locales
Locale Code
-----
en
```

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration status
```

CP ID	CP Name	Mode	Protocol	Verification
1	cp1	Enable	https	Guest
2	cp2	Enable	http	Local
3	cp3	Disable	https	Guest

```
console#show captive-portal configuration 1 status
```

```
CP ID..... 1
CP Name..... cp1
Mode.....
Enabled
Protocol Mode..... https
Verification Mode..... Guest
Group Name.....
group123
Redirect URL Mode.....
Enabled
Redirect URL.....
www.cnn.com
Session Timeout (seconds)..... 86400
```

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

```
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

```
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

```
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 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 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
```


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 pre-requisites 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 Chapter

This chapter explains the following commands:

macro name	macro apply
macro global apply	macro trace
macro global trace	macro description
macro global description	show parser macro

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*

Parameter Description

Parameter	Description
name	The name of the macro. A macro name can consist of any printable characters, including blanks. 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:

Macro	Default Definition
default global	:profile-global
default interface	:profile-desktop
default interface	:profile-phone
default interface	:profile-switch
default interface	:profile-router
default interface	:profile-wireless
default global	:profile-compellent-nas

Command Mode

Global Configuration mode

User Guidelines

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]
```

Parameter Description

Parameter	Description
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]
```

Parameter Description

Parameter	Description
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 (\$).

Parameter	Description
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`

Parameter Description

Parameter	Description
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*]

Parameter Description

Parameter	Description
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*

Parameter Description

Parameter	Description
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*

Parameter Description

Parameter	Description
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 in Privileged EXEC mode to display information about defined macros.

Syntax

show parser macro [*brief* / *description* [*interface interface-id*] / *name macro*

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Clock Commands

Real-time Clock

The PowerConnect 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. PowerConnect 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 Chapter

This chapter explains the following commands:

<code>show sntp configuration</code>	<code>sntp trusted-key</code>
<code>show sntp server</code>	<code>sntp unicast client enable</code>
<code>show sntp status</code>	<code>clock timezone hours-offset</code>
<code>sntp authenticate</code>	<code>no clock timezone</code>
<code>sntp authentication-key</code>	<code>clock summer-time recurring</code>
<code>sntp broadcast client enable</code>	<code>clock summer-time date</code>
<code>sntp client poll timer</code>	<code>no clock summer-time</code>
<code>sntp server</code>	<code>show clock</code>

show sntp configuration

Use the `show sntp configuration` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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.
```

```
Unicast clients: Disable
```

```
Unicast servers:
```

Server	Key	Polling	Priority
-----	-----	-----	-----
10.27.128.21	Disabled	Enabled	1

show sntp server

Use the show sntp server command in Privileged EXEC mode to display the pre-configured SNTP servers. The configured servers can be either IPv4 or IPv6 format.

Syntax

```
show sntp server
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

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
```

```
--More-- or (q)uit
```

```
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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

The following example shows the status of the SNTP.

```
console#show sntp status
```

```
Client Mode:                               Unicast
Last Update Time:                          MAR 30 21:21:20 2009
```

```
Unicast servers:
```

Server	Status	Last response
-----	-----	-----

192.168.0.1	Up	21:21:20 Mar 30 2009

sntp authenticate

Use the **sntp 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

```
sntp authenticate
```

```
no sntp 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(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(config)# sntp authentication-key 8 md5 ClkKey
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

```
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

`sntp client poll timer seconds`

`no sntp client poll timer`

- *seconds* — Polling interval. (Range: 64-1024 seconds, in powers of 2)

Default Configuration

The 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}`

`no sntp server {ip-address | ipv6-address | hostname}`

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters)

Parameter Description

This command does not require a parameter description.

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 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 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 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

```
console(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

```
console(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 {date | month} {month | date} year hh:mm {date | month} {month | date} year hh:mm [offset offset] [zone acronym]` 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 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 2007  
02:00 28 Oct 2007 offset 90 zone EST
```

or

```
console(config)# clock summer-time date Apr 1 2007  
02:00 Oct 28 2007 offset 90 zone EST
```

no clock summer-time

Use the `no clock summer-time` command to reset the summertime configuration.

Syntax Description

`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 in Privileged EXEC or User EXEC mode 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 Description

```
show clock [detail]
```

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

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 2005
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 2005
```

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 2002
```

```
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 Chapter

This chapter explains the following commands:

<code>script apply</code>	<code>script show</code>
<code>script delete</code>	<code>script validate</code>
<code>script list</code>	—

script apply

Use the `script apply` command in Privileged EXEC mode 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 in Privileged EXEC mode 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 in Privileged EXEC mode 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 in Privileged EXEC mode 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#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 in Privileged EXEC mode 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 PowerConnect 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 PowerConnect switch.
- 4 Apply it to the PowerConnect system. With this feature in place, the PowerConnect administrator has the flexibility of creating configuration scripts and then applying the scripts to several devices.

Commands in this Chapter

This chapter explains the following commands:

boot system	filedescr
clear config	rename
copy	show backup-config
delete	show bootvar

delete backup-config	show running-config
delete backup-image	show startup-config
delete startup-config	update bootcode
dir	write
erase	—

boot system

Use the **boot system** command in Privileged EXEC mode to specify the system image that the device loads at startup.

Syntax

```
boot system [unit-id][image1 | image2][active | backup]
```

Parameter Description

The **image1** and **image2** keywords are deprecated on the PC81xx only.

Parameter	Description
image1	Marks the given image as active for subsequent reboots.
image2	Marks the given image as active for subsequent reboots.
unit	Unit to be used for this operation. If absent, command executes on this node.
active	Boot from the currently active image. (PC81xx only)
backup	Boot from the backup image. (PC81xx only)

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 #1

The `image1` and `image2` keywords are deprecated on the PC81xx only. The following example loads system image `image1` for the next device startup.

```
console# boot system image1
```

Example #2

The following example applies to PC81xx only.

```
console #boot system ?
```

`active` Marks the given image as active for subsequent reboots.

`backup` Marks the given image as active for subsequent reboots.

```
console#show version
```

```
Image Descriptions
```

```
active :
```

```
backup :
```

```
Images currently available on Flash
```

unit	active	backup	current-active	next-active
1	<none>	<none>		
2	5.0.0.7	5.0.0.9	5.0.0.7	5.0.0.9

clear config

Use the `clear config` command in Privileged EXEC mode 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 in Privileged EXEC mode to copy files within the switch and to upload and download files from and to the switch.

Syntax

`copy source-url destination-url`

Parameter Description

Parameter	Description	
<i>source-url</i>	The location URL or reserved keyword of the source file being copied. (Range: 1-160 characters.)	
	List of valid source parameters for uploading from the switch:	
	backup-config	Uploads Backup Config file.
	image	Uploads code file by xmodem or tftp.
	operational-log	Uploads Operational Log file.
	running-config	Copies system config file.
	script	Uploads Configuration Script file.
	startup-config	Uploads Startup Config file.
	startup-log	Uploads Startup Log file.
	Valid source URLs for downloading to the switch:	
	xmodem	
	<i>tftp://{ipaddress hostname}/filepath/filename</i> <i>scp://{user@ipaddress hostname}/filepath/filename</i> <i>sftp://{user@ipaddress hostname}/filepath/filename</i> <i>ftp://{user@ipaddress hostname}/filepath/filename</i> <i>flash://filename</i> <i>usb://filepath/filename</i>	

Parameter	Description	
<i>destination-url</i>	The URL or reserved keyword of the destination file. (Range: 1-160 characters.)	
	List of valid destination parameters for downloading to the switch:	
	backup-config	Downloads config file using xmodem, sftp, or tftp.
	image	Downloads code file by xmodem, ftp, sftp, or tftp.
	script	Downloads configuration script by xmodem, sftp, or tftp.
	startup-config	Downloads config file using xmodem or tftp.
	ias-users	Downloads the ias-users database file.
	Valid destination URLs for uploading from the switch:	
	xmodem	
	<i>tftp://{ipaddress hostname}/filepath/filename</i> <i>scp://{user@ipaddress hostname}/filepath/filename</i> <i>sftp://{user@ipaddress hostname}/filepath/filename</i> <i>flash://filename</i> <i>usb://filename/filename</i>	

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.
- *filename*— The name of the file on the server.
- *username*— The user name for logging into the remote server via SSH.

The following table lists and describes reserved keywords.

Reserved Keyword	Description
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
startup-log	Represents the startup syslog file. This can only be the source of a copy operation.
operational-log	Represents the operational syslog file. This can only be the source of a copy operation.
script <i>scriptname</i>	Represents a CLI script file.
image	Represents the software image file. When "image" is the target of a copy command, it refers to the backup image. When "image" is the source of a copy command, it refers to the active image. If this is destination, the file will be distributed to all units in the stack.
ftp:	Source or destination URL for an FTP network server. The syntax for this alias is <code>ftp://ipaddr/filepath/filename image</code> .
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is <code>tftp:[[//location]/directory]/filename</code> . An out-of-band IP address can be specified as described in the User Guidelines.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
usb:	Source or destination URL for a file on a mounted USB file system. Sub-directories are not supported on USB devices.
flash:	Source or destination URL for the switch flash-based file system.
backup-config	Represents the backup configuration file.
unit	Indicates which unit in the stack is the target of the copy command.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

When copying files from the switch, match a source parameter with a destination URL. When copying to the switch, match a source URL to a destination parameter. FTP is only supported for image download to the switch. URLs may not exceed 160 characters in length, including filename, file path, hostname, ip address, user, and reserved keywords.

Examples

Example – Backing up the running-config

```
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#copy tftp://10.27.65.61/PC7000v20100911_2.stk
image
```

```
Transfer Mode..... TFTP
```

```
Server IP Address.....
10.27.65.61
```

```
File Path..... ./
```

```
File Name.....
PCM7000v20100911_2.stk
```

```
Data Type..... Code
```

```
Local Filename..... image
```

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) y

TFTP code transfer starting

9392640 bytes transferred...

File contents are valid.

File transfer operation completed successfully.

console#show bootvar

Image Descriptions

image1 : default image

image2 :

Images currently available on Flash

```
-----  
-----  
unit      image1      image2      current-active  
next-active
```

```
-----  
-----  
  
1      M.9.11.2      M.9.11.3 image1      image1
```

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 – 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 image usb://image1.stk
console#copy flash://crashdump.0 usb://crashdump.0
```

delete

Use the **delete** command to delete files from flash.

Syntax

```
delete file
```

- *file* — Name of the file to be deleted.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#delete file1.scr
Delete file1.scr (Y/N)?y
```

delete backup-config

Use the `delete backup-config` command in Privileged EXEC mode to delete the backup-config file.

Syntax

```
delete backup-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 deletes the backup-config file.

```
console#delete backup-config
Delete backup-config (Y/N)?y
```

delete backup-image

Use the `delete backup-image` command in Privileged EXEC mode to delete a file from a flash memory device.

Syntax

```
delete backup-image
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines



NOTE: The active image cannot be deleted.

Example

The following example deletes test file in Flash memory.

```
console#delete backup-image
```

```
Delete: image2 (y/n)?
```

delete startup-config

Use the `delete startup-config` command in Privileged EXEC mode to delete the startup-config file.

Syntax

```
delete startup-config
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the startup-config file is not present when system reboots, it reboots with default settings.

Example

The following example deletes the startup-config file.

```
console# delete startup-config
```

```
Delete startup-config (y/n)?
```

dir

Use the `dir` command to print the contents of the flash file system.

Syntax

dir

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#dir
  0  drwx          2048 Jan 13 2031 17:19:54 .
  0  drwx          2048 Jan 10 2031 15:58:10 ..
  0  -rwx           256 Jan 22 2005 08:00:48 vpd.bin
  0  -rwx         16380 Jan 10 2031 15:58:18 log2.bin
  0  -rwx           72 Jan 10 2031 15:58:14 boot.dim
  0  -rwx           0 Jan 10 2031 15:58:18 slog2.txt
  0  -rwx         53205 Jan 22 2005 09:45:04 rc.soc
  0  -rwx          148 Jan 10 2031 15:58:22 hpc_broad.cfg
  0  -rwx         11224 Jan 22 2005 09:45:04 helixmem.soc
--More-- or (q)uit
console#
```

erase

Use the `erase` command to erase the startup configuration, the backup configuration, or the backup image.

Syntax

```
erase {startup-config | backup-image | backup-config}
```


Syntax Description

Parameter	Description
startup-config	Erases the contents of the startup configuration file.
backup-image	Erase the backup image.
backup-config	Erases the backup configuration.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

filedescr

Use the **filedescr** command in Privileged EXEC mode to add a description to a file. Use the **no** version of this command to remove the description from the filename.

Syntax

```
filedescr {image 1 | image2} description
```

```
no filedescr {image 1 | image2}
```

- **image1 | image2** — Image file.
- ***description*** — Block of descriptive text. (Range: 0-128 characters)

Default Configuration

No description is attached to the file.

Command Mode

Privileged EXEC mode

User Guidelines

The description accepts any printable characters except a double quote or question mark. Enclose the string in double quotes to include spaces within the name. 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.

Example

The following example attaches a file description to image2.

```
console#filedescr image2 "backedup on 03-22-05"
```

rename

Use the **rename** command in Privileged EXEC mode 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

This command has no user guidelines.

Example

```
console#rename file1.scr file2.scr
```

show backup-config

Use the `show backup-config` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example shows backup-config data.

```
console#show backup-config
software version 1.1
hostname device
interface gigabitethernet 1/0/1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000
exit
interface gigabitethernet 1/0/2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

exit

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, Config mode and all Config sub-modes

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>show bootvar
```

```
Image Descriptions
```

```
image1 : default image
```

```
image2 :
```

```
Images currently available on Flash
```

```
-----  
unit      image1      image2      current-active  next-active  
-----  
1         0.31.0.0    0.31.0.0    image2          image2
```

show running-config

Use the **show running-config** command in Privileged EXEC mode to display the contents of the currently running configuration file, including banner configuration. The command only displays the configurations that are non-default.



NOTE: All non-default configurations for the Captve 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* | *scriptname*]

- *all*—To display or capture the commands with settings and configuration that are equal to the default value, include the *all* option.
- *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

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console# show running-config
...
line ssh
```

```
no exec-banner
exit
line telnet
no login-banner
exit
banner exec "===exec====="
banner login "===login====="
banner motd "===motd====="
exit
```

show startup-config

Use the `show startup-config` command in Privileged EXEC mode to display the startup configuration file contents.

Syntax

```
show startup-config
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the contents of the startup-config file.

PC8024 switch example.

1 : !Current Configuration:

2 : !System Description "Powerconnect 8024F, 4.1.0.6, VxWorks 6.6"

3 : !System Software Version 4.1.0.6

4 : !Cut-through mode is configured as disabled

5 : !

6 : configure

7 : vlan database

8 : vlan 3,1000-1001

9 : vlan routing 1001 1

10 : vlan routing 3 2

11 : exit

12 : stack

13 : member 1 2 ! PC8024F

14 : exit

15 : interface vlan 3

16 : exit

17 : interface vlan 1001

18 : ip address dhcp

19 : exit

20 : username "lv17" password 5f4dcc3b5aa765d61d8327deb882cf99 privilege
15 encrypted

21 : !

22 : interface Tel1/0/3

23 : channel-group 1 mode active

24 : exit

25 : !

26 : interface Tel1/0/4

27 : channel-group 1 mode active

```
28 : exit
29 : !
30 : interface Te1/0/17
31 : switchport mode general
32 : switchport general pvid 1001
33 : switchport general allowed vlan add 1000-1001
34 : switchport general allowed vlan remove 1
35 : exit
36 : snmp-server community "public" rw
37 : exit
```

update bootcode

The `update bootcode` command is deprecated on the PCS1xx only.

Use the `update bootcode` command in Privileged EXEC mode 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

If *unit* is not specified, all units are updated.

Example

The following example updates the bootcode on unit 2.


```
console#update bootcode 2
```

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

Usage Guidelines

This command is equivalent to the `copy running-config startup-config` command functionally.

Example

```
console#write  
console#
```


Denial of Service Commands

The following list shows the DoS attack detection PowerConnect supports. Some platforms do not support detection for all of the DoS attack types in the list.

- SIP=DIP:
 - Source IP address = Destination IP address.
- First Fragment:
 - TCP Header size smaller than 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 Chapter

This chapter explains the following commands:

<code>dos-control firstfrag</code>	<code>ip icmp error-interval</code>
<code>dos-control icmp</code>	<code>ip unreachable</code>
<code>dos-control l4port</code>	<code>ip redirects</code>
<code>dos-control sipdip</code>	<code>ipv6 icmp error-interval</code>
<code>dos-control tcpflag</code>	<code>ipv6 unreachable</code>
<code>dos-control tcpfrag</code>	<code>show dos-control</code>
<code>ip icmp echo-reply</code>	–

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(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
```

```
no 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
```

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

User Guidelines

There are no user guidelines for this command.

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

User Guidelines

There are no user guidelines for this command

Example

```
console(config)#ip icmp error-interval 1000 20
```

ip unreachable

Use the **ip unreachable** 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 unreachable

no ip unreachable

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 icmp unreachable
```

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

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan10)#ip redirects
```

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 unreachablees

Use the **ipv6 unreachablees** 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 unreachablees
```

```
no ipv6 unreachablees
```

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 unreachablees
```

show dos-control

Use the **show dos-control** command in Privileged EXEC mode to display Denial of Service configuration information.

Syntax

```
show dos-control
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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
```

Line Commands

This chapter explains the following commands:

exec-timeout	line
history	show line
history size	speed

Authentication commands related to line configuration mode are in [AAA Commands](#).

exec-timeout

Use the `exec-timeout` command in Line Configuration mode to set the interval that the system waits for user input before timeout. The `exec-timeout` command is also used by the web for timing out web sessions. 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 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.

```
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

Parameter Description

Parameter	Description
<i>number-of-commands</i>	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(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.

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)#
```

show line

Use the **show line** command in User EXEC or Privileged EXEC modes 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the line configuration.

```
console>show line
```

```
Console configuration:
```

```
Interactive timeout: Disabled
```

```
History: 10
```

```
Baudrate: 9600
```

```
Databits: 8
```

```
Parity: none
```

```
Stopbits: 1
```

```
Telnet configuration:
```

```
Interactive timeout: 10 minutes 10 seconds
```

```
History: 10
```

```
SSH configuration:
```

Interactive timeout: 10 minutes 10 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.

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
```

Management ACL Commands

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.

When a Management ACAL is enabled, incoming TCP packets initiating a connection (TCP SYN) and all 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 to the management interface. When the component is disabled, incoming TCP/UDP packets are not filtered and are processed normally.

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 is enabled, the systems management interface is only accessible via the serial port. All TCP SYN packets and UDP packets are dropped except UDP packets sent to the DHCP Server or DHCP Client ports.

Commands in this Chapter

This chapter explains the following commands:

[deny \(management\)](#)

[permit \(management\)](#)

[management access-class](#)

[show management access-class](#)

[management access-list](#)

[show management access-list](#)

deny (management)

Use the **deny** command in Management Access-List Configuration mode to set conditions for the management access list.

Syntax

```
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**, **fttp**, **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 management connections. To disable restriction, 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

This command has no user guidelines.

Example

The following example configures an access-list called *mlist* as the management access-list.

```
console(config)# management access-class 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 for configuration. Once in the access-list configuration mode, the denied or permitted 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

This command enters the access-list configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined.

If no match criteria are defined the default is **deny**.

If reentering to an access-list context, the new rules are entered at 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.

Examples

The following example shows how to configure two management interfaces, gigabit Ethernet 1/0/1 and gigabit Ethernet 2/0/9.

```
console(config)#management access-list mlist
console(config-macal)# permit gigabitethernet 1/0/1
priority 1
console(config-macal)# permit gigabitethernet 2/0/9
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 2/0/9.

```
console(config)# management access-list mlist
console(config-macal)# deny gigabitethernet 1/0/1
priority 1
console(config-macal)# deny gigabitethernet 2/0/9
priority 2
console(config-macal)# permit priority 2
console(config-macal)# exit
console(config) # management access-class mlist
```

permit (management)

Use the **permit** command in Management Access-List configuration mode to set conditions for the management access list.

Syntax

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 1-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. 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. Ensure that each rule has a unique priority.

Examples

The following example shows how to configure two management interfaces, gigabit Ethernet 1/0/1 and gigabit Ethernet 2/0/9.

```
console(config)#management access-list mlist
console(config-macal)# permit gigabitethernet 1/0/1
priority 1
console(config-macal)# permit gigabitethernet 2/0/9
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 2/0/9.

```
console(config)# management access-list mlist
console(config-macal)# deny gigabitethernet 1/0/1
priority 1
console(config-macal)# deny gigabitethernet 2/0/9
priority 2
console(config-macal)# permit priority 2
console(config-macal)# exit
console(config)# management access-class mlist
```

show management access-class

Use the `show management access-class` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the management access-list information.

```
console# show management access-class
```

```
Management access-class is enabled, using access list  
m1ist
```

show management access-list

Use the `show management access-list` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the active management access-list.

```
console# show management access-list
m1ist
-----
permit priority 1 gigabitethernet 1/0/1
permit priority 2 gigabitethernet 2/0/1
! (Note: all other access implicitly denied)
```


Mode Commands

This chapter explains the following commands:

`configure terminal`

`do`

configure terminal

Use the `configure terminal` command to get to the configure line. This command is equivalent to the `configure` command.

Syntax

`configure terminal`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

Example

```
console#conf t
console (config) #
```

```
console#configure terminal
console (config) #
```

do

Use the `do` command to execute commands available in Privileged EXEC mode, Global Configuration and any config sub-mode with command completion. Command completion using the space bar is not available when

using this command. When in modes other than Global Configuration mode, the **do** command will not appear in the list of commands shown in the help, nor will prompting be available.

Syntax

do *line*

do ?

- *line*— Command to be executed. It should 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 except Privileged EXEC and User EXEC modes.

User Guidelines

As per each command.

Example #1

```
console>en
console#configure
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#d?
description                dhcp                do
dot1x                      duplex              dvlan-tunnel
console(config-if-Gi1/0/1)#do ?    ! Help from privileged
EXEC level

console(config)#do ?
```


arp	Purge a dynamic or gateway ARP entry.
boot next reload.	Select a boot image for use on the
captive-portal	Manage captive portal clients.
clear statistics.	Clear learned configuration or
configure	Enter global config mode.
copy	Copy files to or from the switch.
crypto	Request a crypto certificate.
debug	Configure debug flags.
delete	Delete a file.
dir	Display directory information.
disconnect	Close active remote session(s).
dot1x clients.	Initialize dot1x or re-authenticate
enable	Enter into user privilege mode.
erase	Delete a file.
exit	Exit privileged exec mode.
filedescr file.	Set a text description for an image
help keys.	Display help for various special
locate	Blink the locator LED.
logout changes are lost.	Exit this session. Any unsaved
ping IP address.	Send ICMP echo packets to a specified
quit changes are lost.	Exit this session. Any unsaved
release address.	Release an in-band DHCP assigned

reload stack.	Reload stack or a switch in the
rename	Rename a file.
renew address.	Renew an in-band DHCP assigned
script scripts.	Manage and execute configuration
show operational status.	Show configured settings and
telnet	Open a telnet connection.
terminal	Set per session configuration
test first!.	Test a copper port. Disable EEE modes
traceroute	Trace route to destination.
udld	UDLD protocol commands.
unmount device.	Flush cache and un-mount a USB
write	Copy running configuration to
startup configuration.	

console(config-if-Gi1/0/1)#do a? ! Prompt/command
completion from privileged EXEC level

arp

Password Management Commands

The Password Management component supports the features below. Passwords are masked 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 it must conform to each of the following characteristics:

- 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).

The Password strength feature applies to all login passwords (user, line and enable).

Commands in this Chapter

This chapter explains the following commands for viewing and configuring properties of passwords:

passwords aging	passwords strength minimum special-characters
passwords history	passwords strength max-limit consecutive-characters
passwords lock-out	passwords strength max-limit repeated-characters
passwords min-length	passwords strength minimum character-classes
passwords strength-check	passwords strength exclude-keyword
passwords strength minimum uppercase-letters	enable password encrypted
passwords strength minimum lowercase-letters	show passwords configuration
passwords strength minimum numeric-characters	show passwords result



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

Parameter Description

This command does not require a parameter description.

Default Configuration

The default value is 0.

Command Mode

Global Configuration mode

User Guidelines

A value of 0 days disables password aging.

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`

Parameter Description

This command does not require a parameter description.

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`

Parameter Description

This command does not require a parameter description.

Default Behavior

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 **xxxymm** and user level 15.

```
(config)# username bob password xxxymm level 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

no passwords strength-check

Parameter Description

This command does not require parameter descriptions.

Default Behavior

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
```

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
```

Parameter Description

This command has no effect unless enabled by the **passwords strength minimum character-classes** command.

Default Behavior

The default value is 1.

Command Mode

Global Configuration

User Guidelines

This limit is not enforced unless the **passwords strength minimum character-classes** command is configured with a value greater than 0.

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
```

Parameter Description

This command does not require parameter descriptions.

Default Behavior

The default value is 1.

Command Mode

Global Configuration

User Guidelines

This command has no effect unless enabled by the **passwords strength minimum character-classes** command. This limit is not enforced unless the **passwords strength minimum character-classes** command is configured with a value greater than 0.

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`

Parameter Description

This command does not require parameter descriptions.

Default Behavior

The default value is 1.

Command Mode

Global Configuration

User Guidelines

This command has no effect unless the `passwords strength minimum character-classes` command has been enabled.

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`

Parameter Description

This command does not require parameter descriptions.

Default Behavior

The default value is 1.

Command Mode

Global Configuration

User Guidelines

This limit is not enforced unless the `passwords strength minimum character-classes` command is configured with a value greater than 0.

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`

Parameter Description

This command does not require parameter descriptions.

Default Behavior

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*

no passwords strength max-limit repeated-characters

Parameter Description

This command does not require parameter descriptions.

Default Behavior

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 should 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. for special characters, uppercase characters, lower-case characters, etc. 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

Parameter Description

This command does not require parameter descriptions.

Default Behavior

The default value is 0. This 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 pass. A value of 0 disables the minimum strength checking set by the above commands.

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 (inbetween 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]
```


Parameter Description

This command does not require parameter descriptions.

Default Behavior

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

Example

```
console(config)#passwords strength exclude-keyword  
brcm
```

enable password encrypted

This command is used by an Administrator to transfer the enable password between devices without having to know the password. The *password* parameter must be exactly 128 hexadecimal characters.

Syntax

```
enable password encrypted password
```

Parameter Description

This command does not require parameter descriptions.

Default Behavior

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

show passwords configuration

Use the `show passwords configuration` command in Privileged EXEC mode to display the configured password management settings.

Syntax

`show passwords configuration`

Parameter Description

The following fields are displayed by this command.

Parameter	Description
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.

Parameter	Description
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the command output.

```

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.....	brcm, brcm1, brcm2

show passwords result

Use the `show passwords result` command in Privileged EXEC mode to display the last password set result information.

Syntax

```
show passwords result
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 .....
brcm
Password strength check .....
Enable
Last Password Set Result:
Reason for failure: Could not set user password!
Password should contain at least 4 uppercase letters.
```


PHY Diagnostics Commands

This chapter explains the following commands:

<code>show copper-ports tdr</code>	<code>test copper-port tdr</code>
<code>show fiber-ports optical-transceiver</code>	–

show copper-ports tdr

Use the `show copper-ports tdr` command in Privileged EXEC mode to display the stored information regarding cable lengths.

Syntax

`show copper-ports tdr` [*interface*]

- *interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The copper-related commands do not apply to the stacking, CX-4, or 10GBaseT ports associated with these plug-in modules.

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
1/0/1	OK		
1/0/2	Short	50	13:32:00 23 July 2004
1/0/3	Test has not been performed		
1/0/4	Open	128	13:32:08 23 July 2004
1/0/5	Fiber	-	-

show fiber-ports optical-transceiver

Use the `show fiber-ports optical-transceiver` command in Privileged EXEC mode to display the optical transceiver diagnostics.

Syntax

`show fiber-ports optical-transceiver [interface]`

- *interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

The `show fiber ports` command is only applicable to the SFP combo ports and XFP ports (not the ports on the SFP+ plug-in module).

Examples

The following examples display the optical transceiver diagnostics.

```
console#show fiber-ports optical-transceiver
```


Port TX	Temp LOS	Voltage	Current	Output Power	Input Power
1/0/3	w	OK	E	OK	OK
OK	OK				
1/0/4	OK	OK	OK	OK	OK
E	OK				
1/0/1		Copper			

Temp - Internally measured transceiver temperature

Voltage - Internally measured supply voltage

Current - Measured TX bias current

Output Power - Measured TX output power in milliWatts

Input Power - Measured RX received power in milliWatts

TX Fault - Transmitter fault

LOS - Loss of signal

test copper-port tdr

Use the `test copper-port tdr` command in Privileged EXEC mode to diagnose with Time Domain Reflectometry (TDR) technology the quality and characteristics of a copper cable attached to a port.

Syntax

`test copper-port tdr interface`

- *interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines.

During the test, shut down the port under test unless it is a combo port with an active fiber port.



The maximum distance VCT can function is 120 meters.

Examples

The following example results in a report on the cable attached to port 1/0/3.

```
console#test copper-port tdr 1/0/3
```

```
Cable is open at 64 meters
```

The following example results in a failure to report on the cable attached to port 2/0/3.

```
console#test copper-port tdr 2/0/3
```

```
Can't perform the test on fiber ports
```

RMON Commands

The PowerConnect 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 Chapter

This chapter explains the following commands:

rmon alarm	show rmon collection history
rmon collection history	show rmon events
rmon event	show rmon history
show rmon alarm	show rmon log
show rmon alarms	show rmon statistics

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*

Syntax Description

Parameter	Description
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.

Parameter	Description
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 1.3.6.1.2.1.2.2.1.1.10.5 10
50000 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-1/0/8)#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
```

Parameter Description

Parameter	Description
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 string	A comment describing this event. (Range 0-127 characters)
owner string	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
```

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, Config mode and all Config sub-modes

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:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	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.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute , the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is delta , the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	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.

Field	Description
Rising Threshold	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.
Falling Threshold	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.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

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, Config mode and all Config sub-modes

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:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays all RMON group statistics.

```
console> show rmon collection history
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
1	1/0/1	30	50	50	CLI
2	1/0/1	1800	50	50	Manager

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	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.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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: 1/0/1 interval: 1800
Requested samples: 50      Granted samples: 50
Maximum table size: 270
Time                Octets      Packets      Broadcast  Multicast  %
-----
09-Mar-2005  18:29:32  303595962   357568      3289       7287      19
```

The following example displays RMON Ethernet Statistics history for errors on index number 1.

```
console> show rmon history 1 errors
Sample Set: 1Owner: Me
Interface: 1/0/1interval: 1800
Requested samples: 50Granted samples: 50
Maximum table size: 500 (800 after reset)
```

```
TimeCRCUndersizeOversizeFragmentsJabbers
Align
```

```
09-Mar-2005110490
18:29:32
09-Mar-2005110270
18:29:42
```

The following example displays RMON Ethernet Statistics history for "other" on index number 1.

```
console> show rmon history 1 other
Sample Set: 1 Owner: Me
Interface: 1/0/1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 270
```

```
Time Dropped Collisions
-----
```

```

10-Mar-2005  22:06:00      3          0
10-Mar-2005  22:06:20      3          0

```

The following table describes the significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	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.
%	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	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).
Undersize	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.
Oversize	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.
Fragments	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 (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

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.

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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

```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

show rmon statistics

Use the `show rmon statistics` command in User EXEC mode to display 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays RMON Ethernet Statistics for port 1/0/1.

```
console> show rmon statistics gigabitethernet 1/0/1
Port 1/0/1
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display:

Field	Description
Dropped	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.

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.
Broadcast	The total number of good packets received and directed to the Broadcast address. This does not include Multicast packets.
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	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).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	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).
Jabbers	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).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).

Field	Description
65 to 127 Octets	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).
128 to 255 Octets	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).
256 to 511 Octets	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).
512 to 1023 Octets	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).
1024 to 1518 Octets	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).

SDM Templates Commands

On PowerConnect devices, the total available H/W route entries are divided statically (at compile-time) among IPV4 and IPv6 routes. If a switch is deployed in network environments where no IPv6 routes are needed, then H/W resources allocated for IPv6 routes are unused.

The Switch Performance Optimization feature enables the operator to optimize resources for IPv4 only routing environments depending on the how the switch is used in the network at runtime. The operator can choose between Ipv4-only (where all the routing table entries are reserved for IPv4 Routes) or IPv4/IPv6 (Default) mode.

Commands in this Chapter

This chapter explains the following commands:

[sdm prefer](#)

[show sdm prefer](#)

sdm prefer

Use the **sdm prefer** command in Global Config mode to change the template that will be active after the next reboot. To revert to the default template after the next reboot, use the **no** form of this command.

Syntax

```
sdm prefer {dual-ipv4-and-ipv6 default | ipv4-routing {default | data-center}}
```

Parameter Description

Parameter	Description
dual-ipv4-and-ipv6	This keyword filters subsequent template choices to those that support both IPv4 and IPv6. There is only one such template. It is selected using the keyword default .
ipv4-routing	This keyword filters subsequent template choices to those that support IPv4 and not IPv6. The default IPv4-only template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 4. The data-center template supports increases the number of ECMP next hops to 16 and reduces the number of routes.

Default Configuration

The system defaults to the dual IPv4 and IPv6 template.

Command Mode

Global Config

User Guidelines

SDM templates enable you to reallocate system resources to support a different mix of features. After setting the template, you must reboot in order for the configuration change to take effect.

If you attach a unit to a stack and its template does not match the stack's template, then the new unit will automatically reboot using the template used by other stack members. To avoid the automatic reboot, you may first set the template to the template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use the show sdm prefer command below to see what SDM preference is currently active.

Message Type	Message Description
Error Completion Message	None

show sdm prefer

Use the `show sdm prefer` command in Privileged EXEC mode to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template.

Syntax

```
show sdm prefer [dual-ipv4-and-ipv6 default | ipv4-routing {default | data-center}]
```

Parameter Description

Parameter	Description
dual-ipv4-and-ipv6 default	List the scaling parameters for the template supporting IPv4 and IPv6.
ipv4-routing default	List the scaling parameters for the IPv4-only template maximizing the number of unicast routes.
ipv4-routing data-center	List the scaling parameters for the IPv4-only template supporting more ECMP next hops.

The following table explains the output parameters.

Parameter	Description
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.

Parameter	Description
IPv4 Multicast Routes	The maximum number of IPv4 multicast forwarding table entries.
IPv6 Multicast Routes	The maximum number of IPv6 multicast forwarding table entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

When invoked with no optional keywords, this command lists the currently active template, and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using the **no sdm prefer** command or by deleting the startup configuration, the **show sdm prefer** command lists the default template as the next active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

The following table lists the completion messages.

Message Type	Message Description
Successful Completion Message	Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use the show sdm prefer command to see what SDM preference is currently active.
Error Completion Message	None

Examples

This example shows the current SDM template. The user has not changed the next active SDM template.

```
console# show sdm prefer
```

The current template is the Dual IPv4 and IPv6 template.

```
ARP Entries.....6144
IPv4 Unicast Routes.....8160
IPv6 NDP Entries.....2560
IPv6 Unicast Routes.....4096
ECMP Next Hops.....4
IPv4 Multicast Routes.....1536
IPv6 Multicast Routes.....512
```

Now the user sets the next active SDM template for optimal performance for IPv4 routing.

```
console# configure
```

```
console(config)#sdm prefer ipv4-routing default
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

```
config# show sdm prefer
```

The current template is the Dual IPv4 and IPv6 template.

ARP Entries.....	6144
IPv4 Unicast Routes.....	8160
IPv6 NDP Entries.....	2560
IPv6 Unicast Routes.....	4096
ECMP Next Hops.....	4
IPv4 Multicast Routes.....	1536
IPv6 Multicast Routes.....	512

On the next reload, the template will be the IPv4-routing Default template.

To list the scaling parameters for the data center template, invoke the command with the **ipv4-routing data-center** keywords.

```
config# show sdm prefer ipv4-routing data-center
```

Scaling parameters for the IPv4 data center template:

ARP Entries.....	6144
IPv4 Unicast Routes.....	8160
IPv6 NDP Entries.....	0
IPv6 Unicast Routes.....	0
ECMP Next Hops.....	16
IPv4 Multicast Routes.....	2048
IPv6 Multicast Routes.....	0

Serviceability Tracing Packet 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 utility 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 utility. Configuration of console logging in the syslog utility 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 debug 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 Chapter

This chapter explains the following commands:

debug arp	debug ip igmp	debug ipv6 pimdm	debug rip
debug auto-voip	debug ip mcache	debug ipv6 pimsm	debug sflow
debug clear	debug ip pimdm packet	debug isdp	debug spanning-tree

debug console	debug ip pimsm packet	debug lacp	debug vrrp
debug dot1x	debug ip vrrp	debug mld Snooping	show debugging
debug igmp Snooping	debug ipv6 dhcp	debug ospf	–
debug ip acl	debug ipv6 mcache	debug ospfv3	–
debug ip dvmrp	debug ipv6 mld	debug ping	–



NOTE: Debug commands are not persistent across resets.

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.

Syntax

`debug arp`

`no debug arp`

Default Configuration

ARP packet tracing is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug arp
```

debug auto-voip

Use the **debug auto-voip** command to enable Auto VOIP debug messages.

Use 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

```
debug 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

There are no usage guidelines for this command.

Example

```
console#debug auto-voip
```

debug clear

Use the **debug clear** command to disable all debug traces.

Syntax

```
debug clear
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage 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

```
debug console
```

Default Configuration

Display of debug traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug console
```

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

```
debug 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

There are no usage guidelines for this command.

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

There are no usage guidelines for this command.

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

There are no usage guidelines for this command.

Example

```
console#debug ip  acl 1
```

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

```
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

There are no usage guidelines for this command.

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

There are no usage guidelines for this command.

Example

```
console#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

```
debug 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

There are no usage guidelines for this command.

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

There are no usage guidelines for this command.

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

There are no usage guidelines for this command.

Example

```
console#debug ip pimsm packet
```

debug ip vrrp

Use the **debug ip vrrp** command to enable VRRP debug protocol messages. Use the “no” form of this command to disable VRRP debug protocol messages.

Syntax

```
debug ip vrrp  
no debug ip vrrp
```

Default Configuration

Display of VRRP traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#debug ip vrrp
```

debug ipv6 dhcp

Use the **debug ipv6 dhcp** command in Privileged EXEC mode 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

```
debug ipv6 dhcp
```

```
no debug ipv6 dhcp
```

Parameter Description

This command does not require a parameter description.

Default Configuration

Debugging for the DHCP for IPv6 is disabled by default.

Command Mode

Privileged EXEC

User Guidelines

DHCPv6 client already has packet tracing. This command turns the packet tracing on.

Examples

```
console#debug ipv6 dhcp
```

debug 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

This command has no user guidelines.

Example

```
console#debug ipv6 mcache packet
```

debug 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

There are no usage guidelines for this command.

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 pimdm packet [receive | transmit]

Default Configuration

Display of PIMDMv6 traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ipv6 pimdm 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

debug 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.

Usage Guidelines

There are no usage guidelines for this command.

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.

Usage Guidelines

There are no usage guidelines for this command.

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

debug lacp packet

no debug lacp packet

Default Configuration

Display of LACP traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug lacp packet
```

debug mldsnopping

Use the **debug mldsnopping** 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 mldsnopping packet [receive | transmit]

no debug mld Snooping packet [receive | transmit]

Default Configuration

Display of MLD Snooping traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug mld Snooping
```

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.

Syntax

```
debug ospf packet
```

```
no debug ospf packet
```

Default Configuration

Display of OSPF traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

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.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ospfv3 packet
```

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.

Syntax

```
debug ping packet  
no debug ping packet
```

Default Configuration

Display of ICMP echo traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

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.

Usage Guidelines

There are no usage guidelines for this command.

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.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#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 bpd [**receive** | **transmit**]

no debug spanning-tree bpd [**receive** | **transmit**]

Default Configuration

Display of spanning tree BPDU traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug spanning-tree bpdu
```

debug vrrp

Use the **debug vrrp** command in Privileged EXEC mode 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

This command has no user guidelines.

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, Config mode and all Config sub-modes

Usage Guidelines

Enabled packet tracing configurations are displayed.

Example

```
console #debug arp
```

```
Arp packet tracing enabled.
```

```
console #show debugging
```

```
Arp packet tracing enabled.
```

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 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 Chapter

This chapter explains the following commands:

sflow destination	show sflow agent
sflow polling	show sflow destination
sflow polling (Interface Mode)	show sflow polling
sflow sampling	show sflow polling
sflow sampling (Interface Mode)	–

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, the entity making use of this sFlowRcvrTable entry. The default is an empty string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed 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. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. (Range: 0–4294967295 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 port is 6343.

Command Mode

Global Configuration mode.

User Guidelines

An sflow destination entry must have an owner name defined in order for polling or sampling to be configured. 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. 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

This command has no user guidelines.

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 data source if *rcvr_idx* is valid. 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-1/0/2)#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. 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 expires, 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 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.

The default sampling rate is 0.

The default maximum header size is 128.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

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.

The default sampling rate is 0.

The default maximum header size is 128.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/0/15)#sflow 1 sampler 1500 50
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: MIB Version: 1.3, the version of this MIB. Organization: Dell Corp. Revision: 1.0
IP Address	The IP address associated with this agent.

Example

```
console#show sflow agent
```

```
sFlow Version..... 1.3;Dell Corp.;10.23.18.28
IP Address..... 0.0.0.0
```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Receiver Index	The sFlow Receiver associated with the sampler/poller.
----------------	--

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.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.

Example

```
console# show sflow 2 destination
```

```

Receiver Owner      Time out   Max Datagram Port   IP Address
Index   String          Size
-----
2              0          1400      6343   0.0.0.0

```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Poller Data Source	The sFlowDataSource (unit/slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

Example

```
console# show sflow 1 polling
```

```

Poller          Receiver  Poller
Data Source    Index     Interval
-----
1/0/1          1         0

```

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, Config mode and all Config sub-modes

User Guidelines

The following fields are displayed:

Sampler Data Source	The sFlowDataSource (unit/slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Example

```
console# #show sflow 1 sampling
```

```
Sampler      Receiver  Packet      Max Header
Data Source  Index     Sampling Rate  Size
-----
1/0/1       1         0             128
```


SNMP Commands

The SNMP component provides a machine-to-machine interface for the PowerConnect 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 PowerConnect 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.

Commands in this Chapter

This chapter explains the following commands:

<code>show snmp</code>	<code>snmp-server community-group</code>	<code>snmp-server user</code>
<code>show snmp engineID</code>	<code>snmp-server contact</code>	<code>snmp-server view</code>
<code>show snmp filters</code>	<code>snmp-server enable traps</code>	<code>snmp-server v3-host</code>
<code>show snmp group</code>	<code>snmp-server engineID local</code>	—
<code>show snmp user</code>	<code>snmp-server filter</code>	—
<code>show snmp views</code>	<code>snmp-server group</code>	—
<code>show trapflags</code>	<code>snmp-server host</code>	—
<code>snmp-server community</code>	<code>snmp-server location</code>	—

show snmp

Use the `show snmp` command in Privileged EXEC mode to display the SNMP communications status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the SNMP communications status.

```
Console # show snmp
```

```
Community-String Community-Access View name      IP
address
-----
public             read only      user-view     All
private           read write    Default
  172.16.1.1
private           su            DefaultSuper
  172.17.1.1
```

```
Community-String Group name  IP address
-----
public            user-group   All
```

Traps are enabled.

Authentication trap is enabled.

Version 1,2 notifications

Target Address	Type	Community	Version	UDP		
Filter	TO	Retries		Port name	Sec	
192.122.173.42	Trap	public	2	162	filt1	
15	3					
192.122.173.42	Inform	public	2	162	filt2	
15	3					

Version 3 notifications

Target Address	Type	Username	Security	UDP	Filter	
TO	Retries		Level	Port name	Sec	
192.122.173.42	Inform	Bob	Priv	162	filt31	15
3						

System Contact: Robert

System Location: Marketing

show snmp engineID

Use the **show snmp engineID** command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the SNMP engine ID.

```
console# show snmp engineID
```

```
Local SNMP engineID: 08009009020C0B099C075878
```

show snmp filters

Use the `show snmp filters` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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 in Privileged EXEC mode to display the configuration of groups.

Syntax

```
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, Config mode and all Config sub-modes

User Guidelines

The group name accepts any printable characters except a double quote or 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 examples display the configuration of views.

```
console# show snmp group
```

Name	Security		Views		
	Model	Level	Read	Write	
Notify					
-----	-----	-----	-----	-----	
user-group	V3	Auth-Priv	Default	""	
""					
managers-group	V3	NoAuth-priv	Default		
Default			""		
managers-group	V3	NoAuth-priv	Default	""	""

```
console# show snmp groups user-group
```

Name	Security	Views
------	----------	-------

```

Model      Level      Read      Write
Notify
-----
user-group V3      Auth-Priv Default    ""
""

```

The following table contains field descriptions.

Field	Description
Name	Name of the group
Security Model	SNMP model in use (v1, v2 or v3)
Security Level	Authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.
Views	<ul style="list-style-type: none"> • Read—A string that is the name of the view that enables you only to view the contents of the agent. If unspecified, all the objects except the community-table and SNMPv3 user and access tables are available. • Write—A string that is the name of the view that enables you to enter data and manage the contents of the agent. • Notify—A string that is the name of the view that enables you to specify an inform or a trap.

show snmp user

Use the **show snmp user** command in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

The user name accepts any printable characters except a double quote or 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 # 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 # 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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

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	1.3.6.1.2.1.2.2.1.*.1	Included

show trapflags

Use the `show trapflags` command in Privileged EXEC mode to display the trap settings.

Syntax

`show trapflags [ospf|ospfv3|captive-portal]`

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example #1

```
console#show trapflags
Authentication Flag..... Disable
Auto-copy-sw Flag..... Enable
Dot1q Flag..... Enable
Link Up/Down Flag..... Enable
Maclock violation Flag..... Enable
Multiple Users Flag..... Enable
```



```

Spanning Tree Flag..... Enable
VRRP trap..... Enable
ACL Traps..... Enable
DVMRP Traps..... Disable
OSPFv2 Traps..... Disable
PIM Traps..... Disable
OSPFv3 Traps..... Disable
FIP snooping Traps..... Enable

```

Example #2

```

console#show trapflags ospf
OSPF Traps:
errors:
all.....Disabled
authentication failure.....Enabled
bad packet.....Enabled
config error.....Enabled
virt authentication failure .....Disabled
virt bad packet.....Disabled
virt config error.....Disabled
if-rx: if-rxpacket.....Disabled
lsa: lsamaxage.....Disabled
lsaoriginate.....Disabled
overflow: lsdboverflow.....Enabled
lsdb-approaching-overflow.....Enabled
retransmit:
packets.....Disabled

```

```

virtpackets.....Disabled
rtb: rtb-entryinfo.....Disabled
state-change:
all.....Disabled
if state change.....Enabled
neighbor state change.....Enabled
virtif state change.....Disabled
virtneighbor state change.....Disabled

```

snmp-server community

Use the `snmp-server community` command in Global Configuration mode to set up the community access string to permit access to the SNMP protocol. To remove the specified community string, use the `no` form of this command.

Syntax

```
snmp-server community string {ro | rw | su} [view view-name][ipaddress ipaddress]
```

```
no snmp-server community string
```

Parameter Description

Parameter	Description
string	Permits access to the SNMP protocol. (Range: 1-20 characters)
ro	Indicates read-only access.
rw	Indicates read-write access.
su	Indicates SNMP administrator access.
ipaddress	Specifies the IP address of the management station. If no IP address is specified, all management stations are permitted.
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. Default to read-only access if not specified.

Command Mode

Global Configuration mode

User Guidelines

You can not specify *viewname* for *su*, which has an 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 double quote or 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 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` form of this command.

Syntax

`snmp-server community-group community-string group-name [ipaddress ip-address]`

- *community-string* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- *group-name* — Name of a previously defined group. The group defines the objects available to the community. (Range: 1-30 characters)
- *ip-address* — Management station IP address. Default is all IP addresses.

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*.

Example

The following example maps a community access string `dell_community` to group `dell_group`.

```
console(config)# snmp-server community-group
dell_community dell_group 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, 0 to 160 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 | boot auto-copy-sw | captive-portal *cp-type* | dot1q | dvmrp | link | maclock | multiple-users | ospf *ospftype* | ospfv3 *ospfv3type* | pim | poe | snmp authentication | spanning-tree | stack | vrrp]

no snmp-server enable traps [acl | all | boot auto-copy-sw | captive-portal *cp-type* | dot1q | dvmrp | link | maclock | multiple-users | ospf *ospftype* | ospfv3 *ospfv3type* | pim | poe | snmp authentication | spanning-tree | stack | vrrp]

- cp-type - { all, client-auth-failure, client-connect, client-db-full, client-disconnect }
- 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 | lsd-overflow | lsdapproaching-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 | lsd-overflow | lsd-approaching-overflow } | retransmit {all | packets | virt-packets } | state-change { all | if state change | neighbor state change | virtif state change | virtneighbor state change } }

Parameter Description

Parameter	Description
acl	Enable traps on ACL match events.
all	Enable all traps (not recommended).
boot auto-copy-sw	Enable traps on automatic download of switch software.
captive-portal	Enable captive-portal traps.
dot1q	Enable traps on VLAN configuration failures.
dvmrp	Enable dvmrp traps.
maclock	Enable traps on MAC locking violations.

Parameter	Description
ospf	Enable OSPF event traps.
ospfv3	Enable OSPFv3 event traps.
pim	Enable pim traps (pim-sm and pim-dm).
poe	Enable poe traps.
port-aggregator lag-failover	Enable traps for LAG failover on port-aggregator links.
snmp authentication	Enable snmp authentication traps.
spanning-tree	Enable traps on topology changes.
stack	Enable stack firmware synchronization traps.
vrrp	Enable vrrp traps.

Default Configuration

SNMP authentication, link, multiple-user, spanning-tree, dot1q, mac lock violation, and ACL traps are enabled by default.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

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                                 acl
all                                 Enable/Disable all Traps.
authentication                       To enable the device to send SNMP
traps when
```

	authentication fails.
dvmrp	dvmrp
link Up/Down trap flag.	Enable/Disable switch level Link
multiple-users multiple logins	Enable/Disable sending traps when active.
ospf	Enable/Disable OSPF Traps.
ospfv3	Enable/Disable OSPF Traps.
pim	pim
spanning-tree Tree traps.	Enable/Disable sending Spanning

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 not configured.

Command Mode

Global Configuration mode

User Guidelines

If you want to use SNMPv3, you need to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device. If the SNMPv3 engine ID is deleted, or the configuration file is erased, then SNMPv3 cannot be used. Since the EngineID should 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 `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 destroyed, 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.)
- *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 (*) wildcard 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

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 double quote or 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.

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 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 }
```

Parameter Description

Parameter	Description
host-addr	Specifies the IP address of the host (targeted recipient) or the name of the host. (Range:1-158 characters)
community-string	Specifies a password-like community string sent with the notification operation. (Range: 1-20 characters)
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 characters.)
retries	Maximum number of times to resend an inform request. The default is 3 attempts. (Range: 0-255 characters.)
port	UDP port of the host to use. The default is 162. (Range: 1-65535 characters.)
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 on page 514 and the [ip name-server](#) command on page 516 to enable resolution of DNS host names.

Example

The following example enables SNMP traps for host 192.16.12.143.

```
console(config)# snmp-server host 192.16.12.143
Dell_powerconnect traps v2
```

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

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

This command has no user guidelines.

Example

The following example sets the device location as "New_York".

```
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

```
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] ]
```

```
no snmp-server user username
```

- *username* — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters.)
- *groupname* — Specifies the name of the group to which the user belongs. (Range: 1-30 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 acknowledgements to "informs." (Range: 5-32 characters.)
- **auth-md5** — The HMAC-MD5-96 authentication level.
- **auth-sha** — The HMAC-SHA-96 authentication level.
- *password* — A password. (Range: 1 to 32 characters.)
- **auth-md5-key** — The HMAC-MD5-96 authentication level. Enter a pregenerated MD5 key.
- **auth-sha-key** — The HMAC-SHA-96 authentication level. Enter a pregenerated SHA key.
- *md5-key* — Character string—length 32 hex characters.
- *sha-key* — Character string—length 48 characters.

- **priv-des** — The CBC-DES Symmetric Encryption privacy level. Enter a password.
- **priv-des-key** — The CBC-DES Symmetric Encryption privacy level. The user should enter a pregenerated MD5 or SHA key depending on the authentication level selected.
- *des-key* — The pregenerated DES encryption key. Length is determined by authentication method selected—32 hex characters if MD5 Authentication is selected, 48 hex characters if SHA Authentication is selected.

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 reconfigured.

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 (*) wildcard 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

This command can be entered multiple times for the same view record.

The view name accepts any printable characters except a double quote or 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 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 interface group.

```
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 IPv4 address of the host (targeted recipient).
- *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"`.
- *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

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 double quote or 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 identifies an SNMPv3 host.

```
console(config)# snmp-server v3-host 192.168.0.20
```

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.

SSH Commands

Management access to the switch is supported via telnet, SSH, or the serial console. The PowerConnect 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 PowerConnect.

Commands in this Chapter

This chapter explains the following commands:

<code>crypto key generate dsa</code>	<code>key-string</code>
<code>crypto key generate rsa</code>	<code>show crypto key mypubkey</code>
<code>crypto key pubkey-chain ssh</code>	<code>show crypto key pubkey-chain ssh</code>
<code>ip ssh port</code>	<code>show ip ssh</code>
<code>ip ssh pubkey-auth</code>	<code>user-key</code>
<code>ip ssh server</code>	—

crypto key generate dsa

Use the `crypto key generate dsa` command in Global Configuration mode to generate DSA key pairs for your switch. A key pair is one public DSA key and one private DSA key. Use the `no` form of the command to remove the generated key from the local file system.

Syntax

```
crypto key generate dsa
no 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. If your switch already has DSA 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. DSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

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. Use the `no` form of the command to delete the key from the local file system.

Syntax

```
crypto key generate rsa
```

```
no 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. 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.

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 such as SSH client public keys.

Syntax

```
crypto key pubkey-chain ssh
```

Default Configuration

By default, this command has no public keys configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the SSH Public Key-chain configuration mode.

```
console#configure
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#key-String
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWlAl4kpqIw9GBRon
ZQZxjHKcqKL6rMlQ+ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJK67IOU/zfwO11gkTwm175QR9gHujS6KwG
N2QWXgh3ub8gDjTSqMuSn/Wd05iDX2IExQWu08licg1k02LYciz+Z
4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkmlsh
RE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f
+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg01DnwCAC8Q
h
```

```
console (config-pubkey-key) #exit
```

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: 1–65535)

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.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
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

AAA authentication is independent from this configuration.

Example

The following example enables public key authentication for incoming SSH sessions.

```
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 from 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**.

Example

The following example enables the switch to be configured using SSH.

```
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

Use the **key-string row** command to specify which SSH public key you will configure interactively next. To complete the interactive command, you must enter **key-string row** with no characters.

Examples

The following example shows how to enter a public key string for a user called "bob."

```
console (config) #crypto key pubkey-chain ssh
console (config-pubkey-chain) #user-key bob rsa
console (config-pubkey-key) #key-string
AAAAB3NzaC1yc2EAAAADAQABAAQ=CvTnRwPWl
Al4kpbqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJK67IOU/zfwO1lg
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licg1k02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkmlshRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaTlwefWwX6f+
Rmt5nhhqdatN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint:
a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

```
console (config) #crypto key pubkey-chain ssh
console (config-pubkey-chain) #user-key bob rsa
console (config-pubkey-key) #key-string row AAAAB3Nza
```

```
console(config-pubkey-key)#key-string row C1yc2
```

show crypto key mypubkey

Use the `show crypto key mypubkey` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

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
AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WHTjQDUyggjSQXHVgyqdUby
dxUXEAI DHXcWHVr0R/ak1HDQitBzeEv1vVEToEn5ddLmRhtIgrdKU
JHgBHJV
R2VaSN/WC0IK53j9re4B11AE+O3qAxwJs0KD7cTkVF9I+YdiXeOM8
VE4skkw
AiyLDNVWXgNQ6iat8+8Mjth+PIo5t3HykYUCkD8B1v93nzi/sr4hH
HJCdx7w
```

```
wRW3QtgXaGwYt2rd1r3x8ViAF6B7AKYd8xGVVjyJTD6TjrCRRwQHg  
B/BHsFr
```

```
z/Rl1SYa0vFje1/7/0qaIDSHfHqWhajYkMa4xPOtIye7oqzAOm1b7  
6l28uTB
```

```
luBEoLQ+PKOKMiK8sQ==
```

Fingerprint (hex) :

```
58:7f:5c:af:ba:d3:60:88:42:00:b0:2f:f1:5a:a8:fc
```

Fingerprint (bubbleBabble) : xodob-liboh-heret-tiver-
dyrib-godac-pynah-muzyt-mofim-bihog-cuxyx

show crypto key pubkey-chain ssh

Use the `show crypto key pubkey-chain ssh` command in Privileged EXEC mode to display SSH public keys stored on the switch.

Syntax

```
show crypto key pubkey-chain ssh [username username] [fingerprint bubble-  
bubble | hex]
```

- *username* — Specifies the remote SSH client username. (Range: 1–48 characters)
- **bubble-bubble** — 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, Config mode and all Config sub-modes

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
-----  -----
bob       9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F
1:86
john      98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:8
7:C8
```

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
AAAAB3NzaC1yc2EAAAABIwAAAIEAywqRKTRnexcxcxVUVTeMl+Gkh
imyUDhcTkgEfssLPMsgoXlTwzCE5+97UIIsSRKQQR+pBNl45tCYd
75LUofV
4LP6Lj1Q5Q0w5lBgiqC2MZ/iBHGSsHMAE0lpYtelZprDu4uiZHMuW
ezmdQp9
a1PU4jwQ22Tlcfauq3sqC3FMUoU=
  Fingerprint:
2f:09:e7:6f:c9:bf:ab:04:d4:6f:a0:eb:e8:df:7a:11
```

show ip ssh

Use the `show ip ssh` command in Privileged EXEC mode to display the SSH server configuration.

Syntax

```
show ip ssh
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

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 Time	User Name SessionTime	Idle
-----	-----	-----
10.240.1.122	John	
	00:00:00	00:00:08

user-key

Use the **user-key** command in SSH Public Key Chain Configuration mode to specify which SSH public key you are configuring manually. To remove a SSH public key, use the **no** form of this command.

Syntax

```
user-key username {rsa | dsa}
```

`no user-key username`

- *username* — Specifies the remote SSH client username. (Range: 1 to 40 characters)
- `rsa` — RSA key
- `dsa` — DSA key

Default Configuration

By default, there are no keys.

Command Mode

SSH Public Key Chain Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob."

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#
```


Syslog Commands

The PowerConnect supports a centralized logging subsystem with support for local in memory logs, crash dump logs, and forwarding messages to syslog servers. All switch components use the logging subsystem. 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

CLI Logged to Local File and Syslog Server

The PowerConnect 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 PowerConnect management interfaces. When the feature is enabled, all CLI commands are logged using the existing logging subsystems. By default, the feature is disabled.

The CLI command logging severity is set to SEVERITY_NOTICE. The logging severity is not modifiable by the administrator.

For example, the CLI log message for the user admin is:

```
<189> JAN 10 18:59:09 10.27.21.22-2  
CMDLOGGER[209809328]: cmd_logger_api.c(83) 367 %%  
CLI:EIA-232:----:configure
```

```
<190> JAN 10 18:59:17 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 369 %%
[CLI:----:EIA-232] Access level of user admin has been
set to 15
```

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> JAN 10 18:58:56 10.27.21.22-2
CMDLOGGER[209809328]: cmd_logger_api.c(83) 361 %%
CLI:10.27.21.22:admin:User admin logged in
```

```
<190> JAN 10 18:58:56 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 362 %%
[CLI:admin:10.27.21.22] User has successfully logged
in
```

The CLI command log subsystem also logs all user log out instances. The format of the log message is:

```
<190> JAN 10 19:01:04 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 382 %%
[CLI:admin:10.27.21.22] User has logged out
```

Commands in this Chapter

This chapter explains the following commands:

clear logging	logging facility
clear logging file	logging on
description (Logging)	logging snmp
level	logging web-session
logging cli-command	port
logging	show logging
logging audit	show logging file
logging buffered	show syslog-servers

clear logging

Use the **clear logging** command in Privileged EXEC mode 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 in Privileged EXEC mode 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

Parameter Description

Parameter	Description
<i>level</i>	The severity level for syslog messages. (Range: emergency, alert, critical, error, warning, notice, info, debug)

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.

Example

The following example sets the syslog message severity level to alert.

```
console(config-logging)#level alert
```

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

```
console(config)#logging cli-command
```

```
console(config)#do show logging
```

Logging is enabled

Console Logging: level warnings. Console Messages: 384
Dropped.

Buffer Logging: level informational. Buffer Messages:
71 Logged,

File Logging: level notActive. File Messages: 385
Dropped.

CLI Command Logging : enabled

Switch Auditing : enabled

Web Session Logging : disabled

SNMP Set Command Logging : disabled

Syslog server hostname logging: informational.
Messages: 0 dropped

Syslog server

a1234567890123456789012345678901234567890123456789012
3456789012 logging: informational. Messages: 0
dropped

170 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 %%
CLI:EIA-232:----:configure

<190> JAN 10 18:59:17 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 369 %%
[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 %%
CLI:EIA-232:----:exit

<189> JAN 10 18:59:22 10.27.21.22-2
CMDLOGGER[209809328]: cmd_logger_api.c(83) 371 %%
CLI:EIA-232:----:telnet 10.27.21.22

<189> JAN 10 18:59:27 10.27.21.22-2
TRAPMGR[209809328]: traputil.c(614) 372 %% Multiple
Users: Unit: 0 Slot: 5 Port: 1

<189> JAN 10 18:59:27 10.27.21.22-2
CMDLOGGER[209809328]: cmd_logger_api.c(83) 373 %%
CLI:10.27.21.22:admin:User admin logged in

<190> JAN 10 18:59:27 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 374 %%
[CLI:admin:10.27.21.22] User has successfully logged
in

<190> JAN 10 18:59:28 10.27.21.22-2
CLI_WEB[209809328]: cmd_logger_api.c(260) 375 %%
[CLI:admin:10.27.21.22] User admin logged in to enable
mode.
```

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 syslogs, use the **no** form of this command.

Syntax

logging {*ip-address* | *hostname*}

no logging {*ip-address* | *hostname*}

- *ip-address* — IP 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”.

Default Configuration

No syslog servers defined.

Command Mode

Global Configuration mode

User Guidelines

Up to eight syslog servers can be used.

The Dell PowerConnect always uses the local7(23) facility in the syslog message. Syslog messages will not exceed 96 bytes in length. Syslog messages use the following format:

```
<130> JAN 01 00:00:06 0.0.0.0-1 UNKN[0x800023]:  
bootos.c(386) 4 %% Event(0xaaaaaaaa)
```

```
| | | | | | | |
```

```
| | | | | | | | | Message
```

```
| | | | | | | |
```

```
| | | | | | | | | Sequence Number
```

```
| | | | | | | |
```



```

|||||Line Number
|||||
|||||File Name
|||||
|||||Thread ID
|||||
|||Component Name
|||
||Stack ID
||
||Host IP Address
|Timestamp
PRI

```

PRI	This consists of the facility code (see RFC 3164) multiplied by 8 and added to the severity. See below for more information on severity.
Timestamp	The system up time. For systems that use SNTP, this is UTC. When time zones are enabled, local time will be used.
Host IP Address	The IP address of the local system.
Stack ID	The assigned stack ID. 1 is used for systems without stacking capability. The top of stack is used to collect messages for the entire stack.
Component Name	Component name for the logging component. Components must use the new APIs in order to enable identification of the logging component. Component UNKN is substituted for components that do not use the new logging APIs.
Thread ID	The thread ID of the logging component.
File Name	The name of the file containing the invoking macro.
Line Number	The line number which contains the invoking macro.

Sequence Number	The message sequence number for this stack component. Sequence numbers may be skipped because of filtering but are always monotonically increasing on a per stack member basis.
Message	An informative message regarding the event.

Example

The following example places the designated server in logging configuration mode.

```
console (config) #logging 192.168.15.1
```

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

Parameter Description

Parameter	Description
<i>severity-level</i>	(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 **info**.

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.

Example

The following example limits syslog messages displayed from an internal buffer based on the severity level "error."

```
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

Parameter Description

Parameter	Description
<i>severity-level</i>	(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 **warnings**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits messages logged to the console based on severity level "alert".

```
console(config)#logging console alert
```

logging facility

Use the **logging facility** command in Global Config mode to configure the facility to be used in log messages.

Syntax

```
logging facility <facility>
```

```
no logging facility
```

Parameter Description

Parameter	Description
facility	The facility that will be indicated in the message. (Range: local0, local1, local2, local3, local4, local5, local6, local7).

Default Configuration

The default value is local7.

Command Mode

Global Config 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 cancel the buffer, use the **no** form of this command.

Syntax

logging file [*severity-level-number* | *type*]

no logging file

Parameter Description

Parameter	Description
<i>severity-level-number</i>	(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 **error**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits syslog messages sent to the logging file based on the severity level "warning."

```
console(config)#logging file warning
```

logging monitor

Use the **logging monitor** command in Global Config 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
```

Parameter Description

Parameter	Description
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 value is **warnings**.

Command Mode

Global Config 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 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

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 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> MAR 24 07:46:07 10.131.7.165-2 UNKN[83102768]:
cmd_logger_api.c(140) 764 %%
WEB:10.131.7.67:<<UNKNOWN>>:EwaSessionLookup :
session[0] created
<133> MAR 24 07:46:07 10.131.7.165-2 UNKN[83102768]:
cmd_logger_api.c(140) 765 %%
WEB:10.131.7.67:admin:User admin logged in
```

port

Use the **port** command in Logging mode to specify the port number of syslog messages. To reset to the default value, use the **no** form of the command.

Syntax

port *port*

no port

Parameter Description

Parameter	Description
port	The port number for syslog messages. (Range: 1-65535)

Default Configuration

The default port number is 514.

Command Mode

Logging 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.

Example

The following example sets the syslog message port to 300.

```
console(config-logging)#port 300
```

show logging

Use the **show logging** command in Privileged EXEC mode to display all logging information, including auditing status.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
console#show logging
Logging is enabled.
Console Logging: level warnings. Console Messages: 1778
Dropped.
Buffer Logging: level informational. Buffer Messages: 983
Logged,
File Logging: level notActive. File Messages: 1783 Dropped.
CLI Command Logging : disabled
Switch Auditing : disabled
Web Session Logging : disabled
SNMP Set Command Logging : disabled
1141 Messages dropped due to lack of resources.
Buffer Log:
<190> JAN 10 16:26:53 0.0.0.0-1 NIM[177745344]:
nim_intf_map_api.c(381) 985 %% nimCheckIfNumber: incorrect
phase for operation
<190> JAN 10 16:26:53 0.0.0.0-1 NIM[177745344]:
nim_intf_map_api.c(381) 986 %% nimCheckIfNumber: incorrect
phase for operation
```

show logging file

Use the `show logging file` command in Privileged EXEC mode to display the state of logging and the syslog messages stored in the logging file.

Syntax

```
show logging file
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and syslog messages sorted in the logging file.

```
console#show logging file
Persistent Logging : enabled
Persistent Log Count : 1
<186> JAN 01 00:00:05 0.0.0.0-1 UNKN[268434928]:
bootos.c(382) 3 %% Event(0xaaaaaaaa)
```

show syslog-servers

Use the `show syslog-servers` command in Privileged EXEC mode to display the syslog servers settings.

Syntax

```
show syslog-servers
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays the syslog server settings.

```
console#show syslog-servers
```

IP address	Port	Severity	Facility	Descrip tion
192.180.2.275	14	Info	local7	7
192.180.2.285	14	Warning	local7	7

terminal monitor

Use the **terminal monitor** command in Privileged EXEC mode to enable the display of logging messages on the terminal.

Syntax

terminal monitor

no terminal monitor

Default Configuration

The default setting is **terminal monitor**.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **terminal monitor** command in Privileged EXEC mode to change the severity of messages displayed on the terminal monitor.

Use the **no terminal monitor** command to disable the display of logging messages on the terminal.

System Management Commands

This chapter explains the following commands:

asset-tag	login-banner	show hardware profile	
banner exec	media-type	show interfaces media-type	show system fan
banner login	member	–	show system temperature
banner motd	motd-banner	show memory cpu	show tech-support
banner motd acknowledge	nsf	show nsf	show users
clear checkpoint statistics	reload	show power-usage-history	show version
cut-through mode	set description	show process cpu	stack
exec-banner	slot	show sessions	stack-port
hardware profile portmode	show banner	show slot	standby
–	show boot-version	show supported cardtype	switch renumber
–	show checkpoint statistics	show supported switchtype	telnet
–	show cut-through mode	show switch	traceroute
locate	–	show system	–

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 double quote or 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 `lqwepot`. Because the `unit` parameter is not specified, the command defaults to the master switch number.

```
console(config)# asset-tag lqwepot
```

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(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 logged in to the switch. 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

```
console(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 M6220 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 M6220 in the Bottom Chassis - 192.168.12.190.  
This unit is located in A2 and is currently under test.  
M6220-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 M6220 in the Bottom Chassis - 192.168.12.190.  
This unit is located in A2 and is currently under test.  
M6220-C1>
```

SSH (xterm):

```
[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 M6220 in the Bottom Chassis - 192.168.12.190.
This unit is located in A2 and is currently under test.
M6220-C1>
```

Telnet:

```
If you need to utilize this device or otherwise make changes
to the configuration, you may contact Kevin at x911.
Press 'y' to continue (within 30 seconds) (y/n) y
```

```
Please, be advised this unit is under test by Kevin.
User:root
Password:*****
Welcome to the M6220 in the Bottom Chassis - 192.168.12.190.
This unit is located in A2 and is currently under test.
M6220-C1>
```

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.

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
```

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

No specific guidelines.

Example

```
console(config)#cut-through mode
```

The mode (enable) is effective from the next reload of Switch/Stack.

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(config-telnet)# no exec-banner
```

hardware profile portmode

Use the **hardware profile portmode** command in Interface Config 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
```

Parameter Description

Parameter	Description
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 Config mode

User Guidelines

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

Host name not configured.

Command Mode

Global Configuration mode

User Guidelines

The hostname may include any printable characters except a double quote or 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.

```
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.

Syntax

This command has no user guidelines.

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.

Example

```
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
```

locate

Use the `locate` command to locate a switch by LED blinking.

Syntax

```
locate [switch unit] [time time]
```

Parameter Description

Parameter	Description
switch <i>unit</i>	If multiple devices are stacked, you can choose which switch to identify.
time <i>time</i>	LED blinking duration in seconds. Range 1-3600 seconds.

Default Configuration

Default value is 20 seconds.

Command Mode

Privileged EXEC

User Guidelines

The LED will blink green 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
```

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
```

media-type

Select the **media-type** command for the interface. This command is only valid on combo ports.

Syntax

```
media-type { auto-select [rj45 | sfp ] | rj45 | sfp }
```

Parameter Description

Parameter	Description
auto-select rj45	Utilize RJ45 media when both media types are active.
auto-select sfp	Utilize the SFP media when both media types are active.
auto-select	Return the selection to the default (auto-select sfp)
rj45	Force connection on the RJ45 port. Power off SFP media port.
sfp	Force connection on the SFP port. Power off RJ45 media port.

Default Configuration

The default is `media-type auto-select sfp`.

Command Mode

Interface Config

User Guidelines

When both media types are connected, the preference as determined by the `auto-select` keyword parameter selects the active media. When the `auto-select` keyword is not specified, the selected media type is powered on and the alternate media type is powered off. Note that when the `auto-select` keyword is used with any media type, the SFP port will remain powered and the laser, if any, will remain on in order to allow connections over the SFP port.

Example

```
! Select the RJ45 port and power off the SFP port
console(config-if-Te1/0/24)#media-type rj45

! Prefer the RJ45 port and leave the SFP port powered
on
console(config-if-Te1/0/24)#media-type auto-select
rj45
```

member

Use the `member` command in Stack Global Configuration mode to pre-configure 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 a 32-bit integer obtained from the [show supported switchtype](#) command.

Default configuration

This command has no defaults.

Command Mode

Stack Global 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
```

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
```

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 Global 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 in User EXEC mode to check the accessibility of the desired node on the network.

Syntax

ping [*ip* | *ipv6*] *ipaddress* | *hostname* [**repeat** *count*] [**timeout** *interval*] [**size** *size*]

- *ipaddress* — IP address to ping (contact).
- *hostname* — Hostname to ping (contact). (Range: 1–158 characters). 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.
- *count* — Number of packets to send (Range: 1–15 packets).
- *interval* — The time between Echo Requests, in seconds (Range: 1–60 seconds).
- *size* — Number of data bytes in a packet (Range: 0–65507 bytes).

Default Configuration

The default count is 4.

The default interval is 3 seconds.

The default size is 0 data bytes.

Command Mode

User EXEC mode, Privileged EXEC mode

User Guidelines

The local VRRP IP address is not pingable.

Examples

The following example displays a ping to IP address 10.27.65.60

```
console#ping 10.27.65.60
```

Pinging 10.27.65.60 with 0 bytes of data:


```
Reply From 10.27.65.60: icmp_seq = 0. time <10 msec.  
Reply From 10.27.65.60: icmp_seq = 1. time <10 msec.  
Reply From 10.27.65.60: icmp_seq = 2. time <10 msec.  
Reply From 10.27.65.60: icmp_seq = 3. time <10 msec.
```

```
----10.27.65.60 PING statistics----
```

```
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip (msec) min/avg/max = <10/<10/<10
```

```
console#
```

The following example displays a ping to yahoo.com.

```
console#ping yahoo.com
```

```
Pinging yahoo.com [66,217,71,198] with 64 bytes of  
data;
```

```
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```

```
----10.1.1.1 PING Statistics----
```

```
4 packets transmitted, 4 packets received, 0% packet  
loss
```

```
round-trip (ms) min/avg/max = 7/8/11
```

reload

Use the **reload** command in Privileged EXEC mode to reload stack members.

Syntax

reload [*stack-member-number*]

Parameter Description

Parameter	Description
stack-member-number	The stack member to be reloaded.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If no unit is specified, all units are reloaded.

Example

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.
```

set description

Use the **set description** command in Stack Global 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 Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays

```
console (config) #stack
console (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 *cardindex* 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:

- PowerConnect 7024
- PowerConnect 7024P
- PowerConnect 7024F
- PowerConnect 7048
- PowerConnect 7048P
- PowerConnect 7048R

- PowerConnect 7048R-RA
- CX4 Expansion Card
- 10GBaseT Expansion Card
- SFP+ Expansion Card

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 in User EXEC mode.

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, Config mode and all Config sub-modes

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 boot-version

The `show boot-version` command is deprecated on the PC81xx only.

Use the `show boot-version` command to display the boot image version details. The details available to the user include the build date and time.

Syntax

```
show boot-version [ unit ]
```

- *unit* — The switch identifier. (Range: 1–12)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC or Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

No specific guidelines.

Example

```
console#show boot-version
unit          Boot Image Version
1            Thu Aug 30 12:01:04 2007
```

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, Config mode and all Config sub-modes

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
```

```
Messages Checkpointed.....6708
Bytes Checkpointed.....894305
Time Since Counters Cleared.....3d 01:05:09
Checkpoint Message Rate.....0.025
msg/sec
Last 10-second Message Rate.....0 msg/sec
Highest 10-second Message Rate.....8 msg/sec
```

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, Config mode and all Config sub-modes

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

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 in Privileged EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

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 interfaces advanced firmware

Use the `show interfaces advanced firmware` command to display the firmware revision of the PHY for a port.

Syntax

`show interfaces advanced firmware interface`

Parameter Description

Parameter	Description
interface	A 10G non-stacking physical interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command is only applicable to 10G non-stacking interfaces.

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 media-type

Use the `show interfaces media-type` command in Privileged EXEC mode to display the configured and active media type for the combo ports.

Syntax

```
show interfaces media-type
```

Parameter Description

Parameter	Description
auto-select rj45	Utilize RJ45 media when both media types are active.
auto-select sfp	Utilize the SFP media when both media types are active.
rj45	Force connection on the RJ45 port. Power off SFP media port.
sfp	Force connection on the SFP port. Power off RJ45 media port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

```
console#show interfaces media-type
```

Port	Configured Media-Type(s)	Active
-----	-----	-----
Te1/0/21	auto-select, SFP preferred	SFP
Te1/0/22	auto-select, SFP preferred	SFP
Te1/0/23	auto-select, SFP preferred	Down
Te1/0/24	auto-select, SFP preferred	Down

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, Config mode and all Config sub-modes

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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
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

Unit	NSF Support
1	Yes
2	Yes
3	Yes

show power-usage-history

Use the **show power-usage-history** command in Privileged EXEC mode 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*

Parameter Description

Parameter	Description
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, Config mode and all Config sub-modes

User Guidelines

There are no user guidelines for this command.

Example

```
console#show power-usage-history unit 1
```

```
Sampling Interval (sec)..... 30
Total No. of Samples to Keep..... 168
Current Power Consumption (mWatts)..... 56172
```

Sample No.	Time Since The Sample Was Recorded	Power Consumption On This Unit (mWatts)	Power Consumption Per Stack (mWatts)
3	0d:00:00:13	56172	56172
2	0d:00:00:43	56172	56172
1	0d:00:01:12	54360	54360

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
```

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
console#show process cpu
```

Memory Utilization Report

```
status      bytes
-----
   free    64022608
   alloc   151568112
```

CPU Utilization:

```
   PID      Name                5 Sec   1 Min   5
Min
-----
   328bb20  tTffsPTask                0.00%   0.00%
0.02%
   3291820  tNetTask                   0.00%   0.00%
0.01%
```

3295410 tXbdService	0.00%	0.00%
0.03%		
347dcd0 ipnetd	0.00%	0.00%
0.01%		
348a440 osapiTimer	1.20%	1.43%
1.21%		
358ee70 bcmL2X.0	0.40%	0.30%
0.12%		
359d2e0 bcmCNTR.0	0.80%	0.42%
0.50%		
3b5b750 bcmRX	0.00%	0.13%
0.12%		
3d3f6d0 MAC Send Task	0.00%	0.07%
0.10%		
--More-- or (q)uit		
3d48bd0 MAC Age Task	0.00%	0.00%
0.03%		
40fdbf0 bcmLINK.0	0.00%	0.14%
0.46%		
4884e70 tL7Timer0	0.00%	0.06%
0.02%		
48a1250 osapiMonTask	0.00%	0.32%
0.17%		
4969790 BootP	0.00%	0.00%
0.01%		
4d71610 dtlTask	0.00%	0.06%
0.05%		
4ed00e0 hapiRxTask	0.00%	0.06%
0.03%		
562e810 DHCP snoop	0.00%	0.00%
0.06%		

58e9bc0	Dynamic ARP Inspection	0.00%	0.06%
0.03%			
62038a0	dot1s_timer_task	0.00%	0.00%
0.03%			
687f360	dot1xTimerTask	0.00%	0.06%
0.07%			
6e23370	radius_task	0.00%	0.00%
0.01%			
6e2c870	radius_rx_task	0.00%	0.06%
0.03%			
7bc9030	spmTask	0.00%	0.09%
0.01%			
7c58730	ipMapForwardingTask	0.00%	0.06%
0.03%			
7f6eee0	tRtrDiscProcessingTask	0.00%	0.00%
0.01%			
b1516d0	dnsRxTask	0.00%	0.00%
0.01%			
b194d60	tCptvPrtl	0.00%	0.06%
0.03%			
b585770	isdptask	0.00%	0.00%
0.02%			
bda6210	RMONTask	0.00%	0.11%
0.11%			
bdb24b0	boxs Req	0.00%	0.13%
0.10%			
c2d6db0	sshd	0.00%	0.00%
0.01%			

--More-- or (q)uit

```
Total CPU Utilization          2.40%    3.62%
3.45%
```

show sessions

Use the `show sessions` command in Privileged EXEC mode to display a list of the open telnet sessions to remote hosts.

Syntax

```
show sessions
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of open telnet sessions to remote hosts.

```
console#show sessions
```

```
User NameConnection fromIdleSession Session
```

```
Time Time Type
```

```
-----
```

```
---- EIA-232 00:00:0000:07:37 Serial
```

```
admin 192.168.1.248 00:00:17 00:00:26 Telnet
```

```
admin 192.168.1.248 00:00:1600:00:32 HTTP
```

```
console#
```

The following table describes the significant fields shown in the display.

Field	Description
Connection	Connection number
Host	Remote host to which the switch is connected through a Telnet session
Address	IP address of the remote host
Port	Telnet TCP port number

show slot

Use the **show slot** command in User EXEC mode to display information about all the slots in the system or for a specific slot.

Syntax

show slot [*slot/port*]

The following table explains the output parameters.

Parameter	Description
Slot	The slot identifier in a slot/port format.
Slot Status	The slot is empty, full, or has encountered an error.
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.

If you supply a value for slot/port, the following additional information appears as shown in the table below.

Parameter	Description
Inserted Card Model Identifier	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.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	The description of the card preconfigured in the slot.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Config mode and all Config sub-modes

User Guidelines

The command has no user guidelines.

show supported cardtype

Use the **show supported cardtype** command in User EXEC mode to display information about all card types supported in the system. 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.

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.

The following table explains the output parameters.

Parameter	Description
Card Index (CID)	The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier	The model identifier for the supported card type.

If you supply a value for *cardindex*, the following additional information appears as shown in the table below.

Parameter	Description
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Config mode and all Config sub-modes

User Guidelines

The CID information is used when pre-configuring cards using the **slot** command.

show supported switctype

Use the **show supported switctype** command in User EXEC mode to display information about all supported switch types.

Syntax

`show supported swichtype` [*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, Config mode and all Config sub-modes

User Guidelines

The switch SID is used when pre-configuring switches in a stack using the `member` command in `config-stack` mode.

Example

The following example displays the information for supported switch types.

```
console>show supported swichtype
```

```

                                                                    Mgmt      Code
SID                Switch Model ID                Pref      Type
-----
-----
```

The following table describes the fields in the example.

Field	Description
Switch Index (SID)	This field displays the index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	This field displays the model identifier for the supported switch type.

Field	Description
Management Preference	This field indicates the management preference value of the switch type.
Code Version	This field displays the code load target identifier of the switch type.

The following example displays the format of the **show supported switchtype** [*switchindex*] command.

```

console#show supported switchtype 1
Switch Type..... 0xd8200001
Model Identifier..... PC8024
Switch Description..... PowerConnect 8024
Expected Code Type..... 0x100b000
Supported Cards:
Slot..... 0
Card Index (CID)..... 2
    Model Identifier..... PowerConnect 8024
console#

```

The following table describes the fields in the example.

Field	Description
Switch Type	This field displays the 32-bit numeric switch type for the supported switch.
Model Identifier	This field displays the model identifier for the supported switch type.
Switch Description	This field displays the description for the supported switch type.

show switch

Use the **show switch** command in User EXEC mode to display information about units in the stack.

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. If there is a stack firmware synchronization (SFS) operation in progress, the switch status will show as **Updating Code**. Both the pre-configured switch type (as set by the **member** command in stack mode) and the actual connected switch type are shown.

The **show switch *unitid*** command shows details of the switch configuration including the SFS last attempt status for the specified unit.

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 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.

Syntax

```
show switch [chassis-mgmt | stack-member-number | stack-ports[counters  
| diag] | stack-standby]
```

Parameter Description

Parameter	Description
<i>unitid</i>	The unit number.
<i>chassis-mgmt</i>	Display chassis management.
<i>stack-member-number</i>	The stack member number.
<i>stack-ports</i>	Display summary stack-port information for all interfaces.
<i>counters</i>	Display summary data counter information for all interfaces.

Parameter	Description
diag	Display front panel stacking diagnostics for each port.
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 modes, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

Example – Stack Status for the Switch

The following example displays stack status information for the switch.

```
console#show switch 1
```

```
Switch..... 1
Management Status..... Management Switch
Switch Type..... 0xd8200002
Preconfigured Model Identifier.... PC8024F
Plugged-in Model Identifier..... PC8024F
Switch Status..... OK
Switch Description..... Powerconnect 8024F
Expected Code Type..... 0x100b000
```

Detected Code Version..... 4.1.0.6
 Detected Code in Flash..... 4.1.0.6
 SFS Last Attempt Status..... None
 CPLD Version..... 3
 Serial Number.....
 Up Time..... 0 days 0 hrs 11 mins 34 secs

console#The following table describes the fields in the example.

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.
Admin Management Preference	This field indicates the administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Management Switch.
Switch Type	This field displays the 32-bit numeric switch type.
Model Identifier	This field displays the model identifier for this switch. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field displays the switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.
Switch Description	This field displays the switch description.
Expected Code Version	This field indicates the expected code version.

Unit	Description
Detected Code Version	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."
Detected Code in Flash	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 pre-configuration, then the code version is "None."
Boot Code Version	This field displays the version of the boot strapping code.
Up Time	This field displays the system up time.

Example – All Units in the Stack

This example displays information about all units in the stack.

```
console>show switch
```

```
Switch      Management   Preconfig   Plugged-
in  Switch    Code
          Status      Model ID    Model
ID      Status    Version
-----
```

```
1          Mgmt
Switch  PCM8024   PCM8024           1.0.0.0
```

Different fields in the display are explained as follows:

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.

Unit	Description
Preconfigured Model Identifier	This field displays the model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Plugged-In Model Identifier	This field displays the model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field indicates the switch status. Possible values for this state are: OK, Unsupported, CodeMismatch, ConfigMismatch, or NotPresent
Code Version	This field indicates the detected version of code on this switch.

Example – Status Parameters for NSF

The **show switch** command is used to display which unit is the management unit and which is the backup unit. Global Status Parameters for NSF are explained as follows:

Parameter	Description	Range	Default
NSF Administrative Status	Whether nonstop forwarding is administratively enabled or disabled	Enabled Disabled	Enabled
NSF Operational Status	Indicates whether NSF is enabled on the stack.	Enabled Disabled	None

Parameter	Description	Range	Default
Last Startup Reason	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.	Power-On Administrative-Move Warm-Auto-Restart Cold-Auto-Restart	None
Time Since Last Restart	Time since the current management card became the active management card. For the backup manager, the value is set to 0d 00:00:00	Time Stamp	0d 00:00:00
Restart in progress	Whether a restart is in progress. A restart is not considered complete until all hardware tables have been fully reconciled.	Yes or No	
Warm Restart Ready	Whether the initial full checkpoint has finished	Yes or No	
Status	Whether the running configuration on the backup unit includes all changes made on the management unit.	Current or Stale	

Parameter	Description	Range	Default
Time Since Last Copy	When the running configuration was last copied from the management unit to the backup unit.	Time Stamp	
Time Until Next Copy	The number of seconds until the running configuration will be copied to the backup unit. This line only appears when the running configuration on the backup unit is Stale.	0 - L7_UNITMGR_CONFIG_COPY_HOLDDOWN	

```
(nsf-stack) #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
```

```

Unit      NSF Support
----      -
1         Yes
2         Yes
3         Yes

```

Per Unit Status Parameters are explained as follows:

Parameter	Description	Range	Default
NSF Support	Whether a unit supports NSF	Yes or No	—

Example – Switch Firmware Stack Status

The following example displays the Switch Firmware stack status information for the switch.

```
console#show switch
```

```

Management Standby Preconfig Plugged-in
Switch Code
SW Switch Status Model ID Model ID
Status Version
-----
1 Mgmt Sw ANFirebolt-48 ANFirebolt-48
OK 4.12.17.37
2 Stack Mbr ANFirebolt-24 ANFirebolt-24
Updating Code 13.4.8.42

```

```
console#show switch 1
```

```
Switch..... 1
```

```

Management Status..... Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference..... Unassigned
Switch Type..... 0xb6340001
Preconfigured Model Identifier.... PCT7048
Plugged-in Model Identifier..... PCT7048
Switch Status..... OK
Switch Description..... PowerConnect 7048
Expected Code Type..... 0x100b000
Detected Code Version..... 5.31.1.46
Detected Code in Flash..... 5.31.1.46
CPLD Version..... 5
SFS Last Attempt Status..... None
Serial Number..... none
Up Time..... 0 days 2 hrs 14
mins 54 secs

```

console#

Example - SDM Templates

This example shows the SDM Mismatch value in the Switch Status field.

console#show switch

```

ManagementStandby PreconfigPlugged-inSwitchCode
SWSwitchStatusModel IDModel IDStatusVersion
-----
1Mgmt SwANFirebolt-48ANFirebolt-48OK2.24.17.48

```


show system

Use the `show system` command in User EXEC mode 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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

show system fan

Use the `show system fan` command in User EXEC or Privileged EXEC mode to explicitly display the fan status.

Syntax

```
show system fan
```

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

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 in User EXEC mode 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, Config mode and all Config sub-modes

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: 89788978
```

```
Serial number: 8936589782
```

```
Asset tag: 7843678957
```

Unit	Service tag	Serial number	Asset tag
----	-----	-----	-----
1	89788978	8936589782	7843678957
2	4254675	3216523877	5621987728

show system power

Use the `show system power` command in User EXEC or Privileged EXEC mode to display information about the system level power consumption.

Syntax

```
show system power
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

```
console#show system power
```

```
console>show system power
```

```
Power Supplies:
```

Unit	Description	Status	Source	Average
Current	Since		Power	Power
Date/Time				(Watts)
(Watts)				
1	SystemOK	AC	206710688	81540
1	MainOK	AC	4489681540	01/10/2031 15:58:46
1	SecondaryNot	presentDC		

show system temperature

Use the `show system temperature` command in User EXEC or Privileged EXEC mode to display information about the system temperature and fan status.

Syntax

```
show system temperature
```

Parameter Description

This command does not require a parameter description.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

Temperature status is indicated as per the following table:

Status	Degrees Celsius
Good	0-50
Medium	51-74
High	75-200

Examples

```
console>show system temperature
```

Temperature Sensors:

Unit	Description	Temperature (Celsius)	Status
1	MAC	33	Good
1	PHY	24	Good

Fans:

Unit	Description	Status
1	Fan 1	OK
1	Fan 2	OK

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 version`
- `show sysinfo`
- `show port all`
- `show isdp neighbors`
- `show logging`
- `show event log`
- `show logging buffered`
- `show running config`
- `show debugging`

Syntax

`show tech-support`

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

Usage Guidelines

Not applicable

Default Value

Not applicable

Example

```
console#show tech-support
```

```
***** Show Version *****
```

```
Switch: 2
```

```
System Description.....  
PowerConnect 6248P, 1.23.0.33  
  
6.5 VxWorks  
Machine Type.....  
PowerConnect 6248P  
Machine Model.....  
PCT6248P  
Serial Number.....  
CN0PK4632829881C0067  
FRU Number..... 1  
Part Number.....  
BCM56314  
Maintenance Level..... A  
Manufacturer.....  
0xbc00  
Burned In MAC Address.....  
00:1E:4F:04:5D:F4  
Software Version.....  
1.23.0.33  
Operating System.....  
VxWorks 6.5
```

Network Processing Device.....
BCM56314_A0
Additional Packages.....
QOS
Multicast
Stacking
Routing

***** Show SysInfo *****

System Location.....
System Contact.....
System Object ID.....
1.3.6.1.4.1.674.10895.3013
System Up Time..... 0
days 0 hrs 11 mins 47 secs
10/100 Ethernet/802.3 interface(s)..... 4
Gig Ethernet/802.3 interface(s)..... 1
10Gig Ethernet/802.3 interface(s)..... 0
Virtual Ethernet/802.3 interface(s)..... 0

MIBs Supported:

--More-- or (q)uit

Selecting More (m) continues the display of output for the show tech-support command.

show users

Use the **show users** command in Privileged EXEC mode to display information about the active users. 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.

Syntax

```
show users [long]
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of active users and the information about them.

```
console#show users
```

Username	Protocol	Location	Profile(s)
-----	-----	-----	-----
admin	Serial	EIA-232	net-admin

```
console#show users accounts
```

UserName	Privilege	Password Aging	Password Expiry date	Lockout
-----	-----	-----	-----	-----
admin	15	---	---	False

```
Administrative Profile(s) : network-admin
user      1      ---      ---      False
Administrative Profile(s) : network-operator

console#
```

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, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Example

The following example displays a system version (this version number is only for demonstration purposes).

```
console>show version

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash
```

```

-----
unit    image1    image2    current-active    next-
active
-----
-----
1       K.3.9.1    0.0.0.0    image1            image1
2       K.3.9.1    0.0.0.0    image1            image1

```

stack

Use the **stack** command in Global Configuration mode to set the mode to Stack Global Config.

Syntax

```
stack
```

Default Configuration

This command has no default mode.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines. If not 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. Stack members that do not match the saved config after a reboot will show a config mismatch and do not join the stack.

Example

The following example sets the mode to Stack Global 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. This command is used to configure Ethernet ports to operate as either stacking or Ethernet ports.

Syntax

```
stack-port {fortygigabitethernet | tengigabitethernet} unit/slot/port {ethernet  
| stack}
```

Default Configuration

By default, Ethernet ports are configured to operate in Ethernet mode.

Command Mode

Stack Configuration mode

User Guidelines

The **clear config** command will 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 when changing between stacking and Ethernet mode.

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 PC81xx switches.

Example

```
console (config-stack) #stack-port tengigabitethernet  
1/0/3 stack
```

```
console (config-stack) #
```

standby

Use the **standby** command to configure the standby 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: 1–6 maximum. 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 Global Configuration

User Guidelines

No specific guidelines.

Examples

```
console (config) #stack
```

```
console (config-stack) #standby 2
```

switch renumber

Use the **switch renumber** command in Global Configuration mode to change the identifier for a switch in the stack. 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 old switch will be *operationally unplugged*.

Syntax

switch *oldunit* **renumber** *newunit*

- *oldunit*— The current switch identifier. (Range: 1–6)
- *newunit*— The updated value of the switch identifier. (Range: 1–6)

Command Mode

Global Configuration mode

User Guidelines

This command is executed on the Management Switch.

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 in Privileged EXEC mode to log into a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1.....*]

Parameter Description

Parameter	Description
<i>ip-address</i>	Valid IP address of the destination host.
<i>hostname</i>	Hostname of the destination host. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, <code>console (config) #snmp-server host "host name"</code>
<i>port</i>	A decimal TCP port number, or one of the keywords from the port table in the usage guidelines (see Port Table below).
<i>keyword</i>	One or more keywords from the keywords table in the user guidelines (see Keywords Table below).

Keywords Table

Options	Description
/debug	Enable telnet debugging mode.
/line	Enable telnet linemode.
/localecho	Enable telnet localecho.
<cr>	Press ENTER to execute the command.
<i>port</i>	Enter the port number. Refer to the following table.

Port Table

Keyword	Description	Port Number
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7

Keyword	Description	Port Number
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Default Configuration

port — Telnet 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
```

```
Esc U sends telnet EL
```

traceroute

Use the **traceroute** command in Privileged EXEC mode to discover the IP routes that packets actually take when traveling to their destinations.

Syntax

```
traceroute [ ip | ipv6 ] ipaddress | hostname [ initTtl initTtl ] [ maxTtl maxTtl ] [ maxFail maxFail ] [ interval interval ] [ count count ] [ port port ] [ size size ] [source {<src-ip-address> |vlan <vlan-id> |loopback <loop-id>}]
```

Parameter Description

Parameter	Description
<i>ipaddress</i>	Valid IP address of the destination host.
<i>hostname</i>	Hostname of the destination host. (Range: 1–158 characters). The command allows spaces in the host name when specified in double quotes. For example, <code>console (config) #snmp-server host "host name"</code>

Parameter	Description
initTtl	The initial time-to-live (TTL); the maximum number of router hops between the local and remote system (Range: 0–255).
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: 0–255).
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: 0–65507 bytes).
src-ip-address	The IPv4 source address to use in the ICMP echo request packets.
vlan	A valid VLAN interface.
loop-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

There are no user guidelines for this command.

Examples

The following example discovers the routes that packets will actually take when traveling to the destination specified in the command.

```
console#traceroute 192.168.77.171
```

```
Tracing route over a maximum of 20 hops
```

1	192.168.21.1	30 ms	10 ms	10 ms
2		*	*	*
3		*	*	*
4		*	*	*
5		*	*	*

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 acknowledgements. 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 M6220 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 M6220 in the Bottom Chassis -  
192.168.12.190. This unit is located in A2 and is  
currently under test.
```

```
M6220-C1>
```

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 M6220 in the Bottom Chassis -  
192.168.12.190. This unit is located in A2 and is  
currently under test.
```

```
M6220-C1>
```

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 M6220 in the Bottom Chassis -
192.168.12.190. This unit is located in A2 and is
currently under test.

```
M6220-C1>
```

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 M6220 in the Bottom Chassis -
192.168.12.190. This unit is located in A2 and is
currently under test.

Commands in this Chapter

This chapter explains the following commands:

ip telnet server disable	show ip telnet
ip telnet port	–

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
```

Parameter Ranges

Not applicable

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines.

Default Value

This feature is enabled by default.

Example

```
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 the switch.

Syntax

`ip telnet port port number`

- *port number*— Telnet TCP port number (Range: 1–65535)

Default Configuration

The default value for the Telnet TCP port is 23.

Command Mode

Global Configuration

Usage Guidelines

The Telnet TCP port should not be set to a value that might conflict with other well-known protocol port numbers used on this switch.

Example

```
console(config)#ip telnet port 45
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, Config mode and all Config sub-modes

Example

```
(console)#show ip telnet
```

```
Telnet Server is Enabled. Port:23
```

Terminal Length Commands

This chapter provides information about terminal length commands.

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 re-entered. Likewise, because the terminal length setting is specific to a session, it is never saved in the config.

Example

```
console#terminal length 50
```


Time Ranges Commands

Time ranges are used with time-based ACLs to restrict their application due to specific time slots.

This chapter explains the following commands:

time-range	periodic
absolute	show time-range

time-range

Use the **time-range** command in Global Configuration mode to create a time range identified by *name*, 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 this command to delete a time-range identified by *name*.

Syntax

time-range *name*

no time-range *name*

Parameter Description

Parameter	Description
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

This command has no default configuration.

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
```

Parameter Description

Parameter	Description
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
```

Parameter Description

Parameter	Description
days-of-the-week	<p>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.</p> <p>This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.</p> <p>Other possible values are:</p> <ul style="list-style-type: none">• daily -- Monday through Sunday• weekdays -- Monday through Friday• weekend -- Saturday and Sunday <p>If the ending days of the week are the same as the starting days of the week, they can be omitted.</p>
time	<p>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.</p> <p>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.</p>

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 in Privileged EXEC mode 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]

Parameter Description

Parameter	Description
Number of Time Ranges	Number of time ranges configured in the system.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range(active/inactive).
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC, Config mode and all Config sub-modes

User Guidelines

This command has no user guidelines.

Examples

```
console#show time-range timeRange_1
```

```
Time Range Name.....  
timeRange_1  
  
Time Range Status.....  
Inactive
```

Entry Number: 1

Absolute End Time..... 12:00
16 Dec 2010

Periodic Entries: 4

Entry Number: 2

Periodic Start Time..... MON
00:00

Periodic End Time..... TUE
12:30

Entry Number: 3

Periodic Start Time..... TUE
13:00

Periodic End Time..... WED
12:00

Entry Number: 4

Periodic Start Time..... WED
12:30

Periodic End Time..... THU
20:00

Entry Number: 5

Periodic Start Time..... SUN
SAT 18:00

--More-- or (q)uit

Periodic End Time..... SUN
SAT 20:00

console#show time-range

Current number of all Time Ranges: 5 Maximum number
of all Time Ranges: 100

Time Range Name	Status	Entry count	Periodic Absolute Entry
timeRange_1 Exists			Inactive 4
timeRange_2 Exists			Inactive 4
timeRange_3 Exists			Inactive 4
timeRange_4 Exists			Inactive 4
timeRange_5	Inactive	4	Exists

User Interface Commands

This chapter explains the following commands:

<code>enable</code>	–
<code>end</code>	–
<code>exit</code>	<code>quit</code>

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 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 get the CLI user control 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

No specific guidelines.

Example

```
console (config) #end
console#end
console>
```

exit

Use the **exit** command to go to the next lower command prompt 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 with 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 PowerConnect 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 PowerConnect instead of the client browser resulting in a more efficient implementation that allows web access while using Radius or TACACS+ for authentication.

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 Chapter

This chapter explains the following commands:

<code>common-name</code>	<code>ip http secure-port</code>
<code>country</code>	<code>ip http secure-server</code>
<code>crypto certificate generate</code>	<code>key-generate</code>
<code>crypto certificate import</code>	<code>location</code>
<code>crypto certificate request</code>	<code>organization-unit</code>
<code>duration</code>	<code>show crypto certificate mycertificate</code>
<code>ip http port</code>	<code>show ip http server status</code>
<code>ip http server</code>	<code>show ip http server secure status</code>
<code>ip http secure-certificate</code>	<code>state</code>

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*

Parameter Description

Parameter	Description
<i>common-name</i>	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.

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 in Global Configuration mode to generate a self-signed HTTPS certificate.

Syntax

```
crypto certificate number generate
```

Parameter Description

Parameter	Description
<i>number</i>	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. This saved information is never displayed to the user or backed up to another switch. If the RSA keys do not exist, the **generate** parameter must be used. 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.

Example

The following example generates a self-signed HTTPS certificate.

```
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-unit
"PowerConnect Networking"
console(config-crypto-cert)#organization-name "Dell,
Inc."
console(config-crypto-cert)#state TX
console(config-crypto-cert)#key-generate
console(config-crypto-cert)#exit
```

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.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another switch).

Example

The following example imports a certificate signed by the Certification Authority for HTTPS.

```
console(config)#crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBI
AkeAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0km
fhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYe
BABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4
MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASKwgdKggc+ggcyGgcls
ZGFwOi8v
L0VByb3h5JTlWU29mdHdhcmU1MjBSb290JTlWQ2VydG1maWVyLENO
PXNlcnZl
-----END CERTIFICATE-----
Certificate imported successfully.
```

Issued to: router.gm.com

Issued by: www.verisign.com

Valid from: 8/9/2005 to 8/9/2005

Subject: CN= router.gm.com, O= General Motors, C= US

Finger print: DC789788 DC88A988 127897BC BB789788

crypto certificate request

Use the **crypto certificate request** command in Privileged EXEC mode 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 export a certificate request 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 generate the keys. Make sure to re-enter the identical values in the certificate request fields.

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.

duration

Use the **duration** command in Crypto Certificate Generation mode to specify the duration.

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 a duration of 50 days that a certification is valid.

```
console(config-crypto-cert)#duration 50
```

ip http port

Use the **ip http port** command in Global Configuration mode to specify the TCP port for use by a web browser to configure the switch. 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 for use by the HTTP server. (Range: 1–65535)

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 100.

```
console(config)#ip http port 100
```

ip http server

Use the `ip http server` command in Global Configuration mode to enable the switch to be configured, monitored, or modified from a browser. 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 has no user guidelines.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip http server
```

ip http secure-certificate

Use the `ip http secure-certificate` command in Global Configuration mode 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
```

Parameter Description

Parameter	Description
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 generated using the `crypto certificate generate` command in Global Configuration mode.

Example

The following example configures the active certificate for HTTPS.

```
console(config)#ip http secure-certificate 1
```

ip http secure-port

Use the `ip http secure-port` command in Global Configuration mode to configure a TCP port for use by a secure web browser to configure the switch. To use the default port, use the `no` form of this command.

Syntax

```
ip http secure-port port-number
```

```
no ip http secure-port
```

Parameter Description

Parameter	Description
<i>port-number</i>	Port number for use by the secure HTTP server. (Range: 1–65535)

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.

Example

The following example configures the HTTPS port number to 100.

```
console(config)#ip http secure-port 2
```

ip http secure-server

Use the **ip http secure-server** command in Global Configuration mode to enable the switch to be configured, monitored, or modified securely from a browser. To disable this function, 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

You must import a certificate using the **crypto certificate import** command, followed by the **crypto certificate generate** command.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip http secure-server
```

key-generate

Use the **key-generate** command in Crypto Certificate Generation mode to specify the key-generate.

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

This command has no default configuration.

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.

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
```

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)

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 "generalmotors" organization-unit.

```
console (config-crypto-cert) #organization-unit  
generalmotors
```

show crypto certificate mycertificate

Use the `show crypto certificate mycertificate` command in Privileged EXEC mode 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, Config mode and all Config sub-modes

Example

The following example displays the SSL certificate of a sample switch.

```
console#show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBI
AkEAp4HS
NnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0km
fhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYe
BABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4
MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASKwgdKggc+ggcyGgc1s
ZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmU1MjBSb290JTIwQ2VydG1maWVyLENO
PXN1cnZl
-----END CERTIFICATE-----
```

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

show ip http server status

Use the `show ip http server` command in User EXEC or Privileged EXEC mode to display the HTTP server status information.

Syntax

`show ip http server status`

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC, Config mode and all Config sub-modes

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 in User EXEC or Privileged EXEC mode to display the HTTP secure server status information.

Syntax

show ip http server secure status

Syntax Description

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC, Privileged EXEC modes, Config mode and all Config sub-modes

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 https
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
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
```

Finger print: 1873B936 88DC3411 BC8932EF 782134BA

The following example displays the HTTPS server configuration with DH Key exchange disabled.

```
console#show ip https
```

```
HTTPS server enabled. Port: 443
```

```
DH Key exchange disabled, parameters are being generated.
```

```
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
```

```
Certificate 2 is inactive
```

```
Issued by: self-signed
```

```
Valid from: 8/9/2003 to 8/9/2004
```

```
Subject: CN= router.gm.com, O= General Motors, C= US
```

```
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

state

Use the **state** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the state or province name.

Syntax

```
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 "texas."

```
console(config-crypto-cert)#state texas
```


Appendix A: List of Commands

A

aaa accounting dot1x default start-stop	709
aaa authentication dot1x default	240
aaa authentication enable	241
aaa authentication login	243
aaa authorization	245
aaa authorization network default radius	247
aaa ias-user username	248
aaa new-model	249
absolute	1786
access-list	282
accounting	711
acct-port	712
action	575
add gigabitethernet	577
add port-channel	578
add tengigabitethernet	577
admin-profile	273
area default-cost (Router OSPF)	1209
area default-cost (Router OSPFv3)	1302
area nssa (Router OSPF)	1210
area nssa (Router OSPFv3)	1303
area nssa default-info-originate (Router OSPF Config)	1212
area nssa default-info-originate (Router OSPFv3 Config)	1304
area nssa no- redistribute	1213, 1305
area nssa no-summary	1214, 1306
area nssa translator-role	1214, 1307
area nssa translator-stab-intv	1215, 1308
area range (Router OSPF)	1216
area range (Router OSPFv3)	1309
area stub	1220, 1310
area stub no-summary	1221, 1311
area virtual-link	1221, 1312
area virtual-link authentication	1224
area virtual-link dead-interval	1225, 1314
area virtual-link hello-interval	1226, 1314

area virtual-link retransmit-interval	1227, 1315
area virtual-link transmit-delay	1228, 1316
arp	956
arp access-list	383
arp cachesize	957
arp dynamicrenew	958
arp purge	959
arp resptime	960
arp retries	961
arp timeout	961
asset-tag	1707
assign-queue	647
authentication timeout	1437
authorization	250
auth-port	713
auto-cost	1229
auto-summary	1375
B	
bandwidth	1230
banner exec	1708
banner login	1709
banner motd	1710
banner motd acknowledge	1711
block	1442
boot auto-copy-sw	1426
boot auto-copy-sw allow-downgrade	1427
boot host autoreboot	1428
boot host autosave	1429
boot host dhcp	1429
boot host retrycount	1430
boot system	1504
bootfile	971
bootpdhcprelay maxhopcount	1053
bootpdhcprelay minwaittime	1054
C	
capability opaque	1230
captive-portal	1437
captive-portal client deauthenticate	1450

channel-group	624
class	647
class-map	648
class-map rename	649
classofservice dot1p-mapping	650
classofservice ip-dscp-mapping	651
classofservice traffic-class-group	901
classofservice trust	654
clear (IAS)	249
clear arp-cache	962
clear arp-cache management	963
clear captive-portal users	1455
clear checkpoint statistics	1714
clear config	1505
clear counters	414
clear dhcp l2relay statistics interface	354
clear dot1x authentication-history	874
clear fip-snooping statistics	943
clear gvrp statistics	475
clear host	508
clear ip address-conflict-detect	508
clear ip arp inspection statistics	384
clear ip dhcp binding	972
clear ip dhcp conflict	973
clear ip dhcp snooping binding	366
clear ip dhcp snooping statistics	367
clear ip helper statistics	1055
clear ip ospf	1231
clear ip ospf stub-router	1232
clear ipv6 dhcp	999
clear ipv6 neighbors	1098
clear ipv6 statistics	1099
clear isdp counters	329
clear isdp table	330
clear lldp remote-data	584
clear lldp statistics	585
clear logging	1687
clear logging email statistics	406
clear logging file	1687

clear mac address-table	298
clear priority-flow-control statistics	949
clear spanning-tree detected-protocols	739
client-identifier	973
client-name	974
clock summer-time date	1492
clock summer-time recurring	1491
clock timezone hours-offset	1490
common-name	1798
compatible rfc1583	1233
configuration	1443
configure terminal	1555
conform-color	655
copy	1506
cos-queue min-bandwidth	656
cos-queue random-detect	657
cos-queue strict	658
country	1799
crypto certificate generate	1800
crypto certificate import	1801
crypto certificate request	1803
crypto key generate dsa	1673
crypto key generate rsa	1674
crypto key pubkey-chain ssh	1675
cut-through mode	1715

D

datacenter-bridging	889
deadtime	713
debug aaa accounting	714
debug arp	1610
debug auto-voip	1611
debug cfm	466
debug clear	1611
debug console	1612
debug dhcp packet	360
debug dot1x	1612
debug igmpsnooping	1613
debug ip acl	1614
debug ip dvmrp	1614

debug ip igmp	1615
debug ip mcache	1616
debug ip pimdm packet	1617
debug ip pimsm packet	1618
debug ip vrrp	1618
debug ipv6 dhcp	1619
debug ipv6 mcache	1620
debug ipv6 mld	1620
debug ipv6 pimdm	1621
debug ipv6 pimsm	1622
debug isdp	1623
debug lacp	1624
debug mldsnopping	1624
debug ospf	1625
debug ospfv3	1626
debug ping	1626
debug rip	1627
debug sflow	1628
debug spanning-tree	1628
debug udld	789
debug vrrp	1629
default-information originate (Router OSPF Configuration)	1234
default-information originate (Router OSPFv3 Configuration)	1317
default-information originate (Router RIP Configuration)	1376
default-metric	1235, 1318, 1377
default-router	975
delete	1513
delete backup-config	1514
delete backup-image	1514
delete startup-config	1515
deny (management)	1546
deny permit (IP ACL)	284
deny permit (IPv6 ACL)	530
deny permit (Mac-Access-List-Configuration)	286
depends-on	579
description	415
description (Administrative Profile Config)	274
description (Logging)	1688
dhcp l2relay (Global Configuration)	341

dhcp l2relay (Interface Configuration)	342
dhcp l2relay circuit-id	343
dhcp l2relay remote-id	344
dhcp l2relay trust	344
dhcp l2relay vlan	345
diffserv	659
dir	1515
distance ospf	1236, 1319
distance rip	1378
distribute-list out	1237, 1378
dns-server (IP DHCP Pool Config)	976
dns-server (IPv6 DHCP Pool Config)	1000
do	1555
domain-name (IP DHCP Pool Config)	977
domain-name (IPv6 DHCP Pool Config)	1000
dos-control firstfrag	1529
dos-control icmp	1529
dos-control l4port	1530
dos-control sipdip	1531
dos-control tcpflag	1532
dos-control tcpfrag	1532
dot1x dynamic-vlan enable	849
dot1x guest-vlan	875
dot1x initialize	850
dot1x mac-auth-bypass	850
dot1x max-req	851
dot1x max-users	852
dot1x port-control	853
dot1x re-authenticate	854
dot1x reauthentication	855
dot1x system-auth-control	855
dot1x system-auth-control monitor	856
dot1x timeout guest-vlan-period	857
dot1x timeout quiet-period	858
dot1x timeout re-authperiod	859
dot1x timeout server-timeout	860
dot1x timeout supp-timeout	860
dot1x timeout tx-period	861
dot1x unauth-vlan	876

drop	660
duplex	416
duration	1804
dvlan-tunnel ethertype	797
E	
enable	1238, 1320, 1379, 1438, 1443, 1793
enable authentication	251
enable password	252
enable password encrypted	1573
encapsulation	1070
end	1794
erase	1516
ethernet cfm cc level	452
ethernet cfm domain	450
ethernet cfm mep active	455
ethernet cfm mep archive-hold-time	456
ethernet cfm mep enable	454
ethernet cfm mep level	453
ethernet cfm mip level	456
exec-banner	1715
exec-timeout	1539
exit	1794
exit (mst)	740
exit-overflow-interval	1239, 1321
external-lsdb-limit	1239, 1322
F	
feature fip-snooping	915
filedescr	1517
fip-snooping enable	916
fip-snooping fc-map	917
fip-snooping port-mode	918
flowcontrol	417
G	
garp timer	476
green-mode eee	471
green-mode eee-lpi-history	472
green-mode energy-detect	470
group	1444

gvrp enable (global)	477
gvrp enable (interface)	478
gvrp registration-forbid	479
gvrp vlan-creation-forbid	480

H

hardware profile portmode	1716
hardware-address	977
hashing-mode	626
history	1540
history size	1541
host	978
hostname	1717
hostroutesaccept	1380
http port	1439
https port	1439

I

initiate failover	1718
instance (mst)	740
interface	418, 1445
interface loopback	1151
interface port-channel	625
interface range	419
interface range port-channel	625
interface range vlan	799
interface tunnel	1392
interface vlan	798
ip access-group	288
ip address	1071
ip address (Out-of-Band)	509
ip address dhcp (Interface Config)	511
ip address-conflict-detect run	510
ip arp inspection filter	385
ip arp inspection limit	386
ip arp inspection trust	387
ip arp inspection validate	387
ip arp inspection vlan	388
ip default-gateway	513
ip dhcp bootp automatic	979

ip dhcp conflict logging	980
ip dhcp excluded-address	981
ip dhcp ping packets	982
ip dhcp pool	968
ip dhcp relay information check	1055
ip dhcp relay information check-reply	1056
ip dhcp relay information option	1057
ip dhcp relay information option-insert	1058
ip dhcp snooping	367
ip dhcp snooping binding	368
ip dhcp snooping database	369
ip dhcp snooping database write-delay	370
ip dhcp snooping limit	371
ip dhcp snooping log-invalid	372
ip dhcp snooping trust	373
ip dhcp snooping verify mac-address	374
ip domain-lookup	514
ip domain-name	514
ip dvmrp	1019
ip dvmrp metric	1020
ip helper enable	1063
ip helper-address (global configuration)	1059
ip helper-address (interface configuration)	1061
ip host	515
ip http authentication	253
ip http port	1804
ip http secure-certificate	1806
ip http secure-port	1807
ip http secure-server	1808
ip http server	1805
ip https authentication	254
ip icmp echo-reply	1533
ip icmp error-interval	1534
ip igmp	1028
ip igmp last-member-query-count	1029
ip igmp last-member-query-interval	1030
ip igmp query-interval	1031
ip igmp query-max-response-time	1032
ip igmp robustness	1032

ip igmp snooping (global)	486
ip igmp snooping (interface)	487
ip igmp snooping (VLAN)	494
ip igmp snooping fast-leave	494
ip igmp snooping groupmembership-interval	495
ip igmp snooping host-time-out	488
ip igmp snooping leave-time-out	488
ip igmp snooping maxresponse	496
ip igmp snooping mcrtreptime	497
ip igmp snooping mrouter-time-out	489
ip igmp snooping querier	499
ip igmp snooping querier election participate	501
ip igmp snooping querier query-interval	502
ip igmp snooping querier timer expiry	503
ip igmp snooping querier version	503
ip igmp startup-query-count	1033
ip igmp startup-query-interval	1034
ip igmp version	1035
ip igmp-proxy	1043
ip igmp-proxy reset-status	1044
ip igmp-proxy unsolicited-report-interval	1045
ip irdp	1365
ip irdp address	1367
ip irdp holdtime	1368
ip irdp maxadvertinterval	1369
ip irdp minadvertinterval	1370
ip irdp multicast	1371
ip irdp preference	1372
ip local-proxy-arp	964
ip mcast boundary	1157
ip mroute	1157
ip mtu	1072
ip multicast	1158
ip multicast ttl-threshold	1159
ip name-server	516
ip netdirbcast	1074
ip ospf area	1240
ip ospf authentication	1241
ip ospf cost	1242

ip ospf database-filter all out	1243
ip ospf dead-interval	1243
ip ospf hello-interval	1244
ip ospf mtu-ignore	1245
ip ospf network	1246
ip ospf priority	1247
ip ospf retransmit-interval	1247
ip ospf transmit-delay	1248
ip pim	1160
ip pim bsr-border	1161
ip pim bsr-candidate	1161
ip pim dense	1163
ip pim dr-priority	1163
ip pim hello-interval	1164
ip pim join-prune-interval	1165
ip pim register-rate-limit	1166
ip pim rp-address	1166
ip pim rp-candidate	1167
ip pim sparse	1168
ip pim spt-threshold	1170
ip pim ssm	1169
ip proxy-arp	964
ip redirects	1535
ip rip	1381
ip rip authentication	1381
ip rip receive version	1382
ip rip send version	1383
ip route	1074
ip route default	1076
ip route distance	1077
ip routing	1078
ip ssh port	1676
ip ssh pubkey-auth	1677
ip ssh server	1677
ip telnet port	1781
ip telnet server disable	1780
ip unreachable	1535
ip verify binding	559
ip verify source	557

ip verify source port-security	558
ip vrrp	1400
ip vrrp accept-mode	1419
ipv6 access-list	532
ipv6 access-list rename	533
ipv6 address	1100
ipv6 address (Interface Config)	517
ipv6 address (OOB Port)	518
ipv6 address dhcp	520
ipv6 dhcp pool	1001
ipv6 dhcp relay	1002
ipv6 dhcp server	1003
ipv6 enable	1101
ipv6 enable (Interface Config)	521
ipv6 enable (OOB Config)	521
ipv6 gateway (OOB Config)	522
ipv6 hop-limit	1102
ipv6 host	1102
ipv6 icmp error-interval	1536
IPv6 Limitations & Restrictions	1097
ipv6 mld last-member-query-count	1103
ipv6 mld last-member-query-interval	1104
ipv6 mld query-interval	1107
ipv6 mld query-max-response-time	1107
ipv6 mld router	1108
ipv6 mld snooping (Global)	543
ipv6 mld snooping (Interface)	544
ipv6 mld snooping (VLAN)	545
ipv6 mld snooping groupmembership-interval	541
ipv6 mld snooping immediate-leave	540
ipv6 mld snooping maxresponse	541
ipv6 mld snooping mcrxexpiretime	542
ipv6 mld snooping querier	550
ipv6 mld snooping querier (VLAN mode)	550
ipv6 mld snooping querier address	551
ipv6 mld snooping querier election participate	552
ipv6 mld snooping querier query-interval	552
ipv6 mld snooping querier timer expiry	553
ipv6 mld-proxy	1105

ipv6 mld-proxy reset-status	1105
ipv6 mld-proxy unsolicit-rprt-interval	1106
ipv6 mtu	1109
ipv6 nd dad attempts	1110
ipv6 nd managed-config-flag	1111
ipv6 nd ns-interval	1111
ipv6 nd other-config-flag	1112
ipv6 nd prefix	1113
ipv6 nd ra-interval	1114
ipv6 nd ra-lifetime	1115
ipv6 nd reachable-time	1116
ipv6 nd suppress-ra	1117
ipv6 ospf	1322
ipv6 ospf area	1323
ipv6 ospf cost	1324
ipv6 ospf dead-interval	1325
ipv6 ospf hello-interval	1326
ipv6 ospf mtu-ignore	1326
ipv6 ospf network	1327
ipv6 ospf priority	1328
ipv6 ospf retransmit-interval	1329
ipv6 ospf transmit-delay	1330
ipv6 pim (Global config)	1185
ipv6 pim (VLAN Interface config)	1186
ipv6 pim bsr-border	1187
ipv6 pim bsr-candidate	1187
ipv6 pim dense	1188, 1195
ipv6 pim dr-priority	1189
ipv6 pim hello-interval	1190
ipv6 pim join-prune-interval	1190
ipv6 pim register-rate-limit	1191
ipv6 pim register-threshold	1192
ipv6 pim rp-address	1193
ipv6 pim rp-candidate	1193
ipv6 pim sparse (Global config)	1194
ipv6 pim spt-threshold	1195
ipv6 pim ssm	1196
ipv6 route	1118
ipv6 route distance	1119

ipv6 router ospf	1331
ipv6 traffic-filter	534
ipv6 unicast-routing	1120
ipv6 unreachable	1537
iscsi aging time	564
iscsi cos	565
iscsi enable	567
iscsi target port	568
isdp advertise-v2	330
isdp enable	331
isdp holdtime	332
isdp timer	333
K	
key	715, 774
key-generate	1808
key-string	1678
L	
lACP port-priority	627
lACP system-priority	628
lACP timeout	629
lease	983
level	1689
line	1541
link-dependency group	576
lldp dcbx port-role	893
lldp dcbx version	890
lldp notification	586
lldp notification-interval	586
lldp receive	587
lldp timers	588
lldp tlv-select dcbx	891
lldp transmit	589
lldp transmit-mgmt	590
lldp transmit-tlv	590
locale	1445
locate	1719
location	1809
log adjacency-changes	1249

logging	1692
logging audit	1694
logging buffered	1694
logging cli-command	1689
logging console	1696
logging email	398
logging email from-addr	403
logging email logtime	404
logging email message-type subject	403
logging email message-type to-addr	402
logging email test message-type	405
logging email urgent	400
logging facility	1697
logging file	1698
logging monitor	1699
logging on	1700
logging snmp	1701
logging traps	401
logging web-session	1701
login authentication	256
login-banner	1719

M

mac access-group	289
mac access-list extended	290
mac access-list extended rename	291
mac address-table aging-time	299
mac address-table multicast filtering	300
mac address-table multicast forbidden address	301
mac address-table multicast forbidden forward-unregistered	303
mac address-table multicast forward-all	304
mac address-table multicast forward-unregistered	305
mac address-table multicast static	306
mac address-table static	307
macro apply	1474
macro description	1476
macro global apply	1471
macro global description	1473
macro global trace	1472
macro name	1470

macro trace	1475
mail-server ip-address hostname	408
management access-class	1547
management access-list	1548
mark cos	661
mark ip-dscp	661
mark ip-precedence	662
match class-map	663
match cos	664
match destination-address mac	665
match dstip	666
match dstip6	667
match dstl4port	667
match ethertype	668
match ip dscp	670
match ip precedence	671
match ip tos	671
match ip6flowlbl	669
match protocol	672
match source-address mac	673
match srcip	674
match srcip6	675
match srcl4port	675
match vlan	676
maximum-paths	1252, 1331
max-metric router-lsa	1250
media-type	1720
member	1721
mirror	677
mode dvlan-tunnel	800
monitor session	640
motd-banner	1722
msgauth	716
mtu	420
mvr	602
mvr group	603
mvr immediate	606
mvr mode	604
mvr querytime	604

mvr type	607
mvr vlan	606
mvr vlan group	609
N	
name (Captive Portal)	1446
name (mst)	742
name (RADIUS server)	716
name (VLAN Configuration)	801
netbios-name-server	984
netbios-node-type	985
network	986
network area	1253
next-server	986
no clock summer-time	1493
no clock timezone	1490
no user	1455
nsf	1254, 1332, 1723
nsf helper	1255, 1333
nsf helper strict-lsa-checking	1256, 1334
nsf restart-interval	1256, 1335
O	
option	987
organization-unit	1810
P	
passive-interface	1258, 1335
passive-interface default	1257, 1336
password (aaa IAS User Configuration)	257
password (Line Configuration)	258
password (Mail Server Configuration Mode)	410
password (User EXEC)	259
passwords aging	1562
passwords history	1562
passwords lock-out	1563
passwords min-length	1564
passwords strength exclude-keyword	1572
passwords strength max-limit consecutive-characters	1569
passwords strength max-limit repeated-characters	1570
passwords strength minimum character-classes	1571

passwords strength minimum lowercase-letters	1567
passwords strength minimum numeric-characters	1568
passwords strength minimum special-characters	1569
passwords strength minimum uppercase-letters	1566
passwords strength-check	1565
periodic	1787
permit (management)	1549
permit ip host mac host	389
ping	1724
ping ethernet cfm	457
ping ipv6	1121
ping ipv6 interface	1122
police-simple	678
policy-map	679
port	774, 1702
port (Mail Server Configuration Mode)	409
port security	308
port security max	309
port-channel local-preference	629
port-channel min-links	630
prefix-delegation	1004
primary	718
priority	718, 775
priority-flow-control mode	946
priority-flow-control priority	947
private-vlan	834
protocol	1447
protocol group	802
protocol vlan group	803
protocol vlan group all	804
Q	
quit	1795
R	
radius-server attribute 4	719
radius-server deadtime	720
radius-server host	721
radius-server key	722
radius-server retransmit	723

radius-server source-ip	724
radius-server timeout	724
random-detect exponential-weighting-constant	682
random-detect queue-parms	680
redirect	683, 1447
redirect-url	1448
redistribute	1259, 1337, 1384
release dhcp	358
reload	1725
rename	1518
renew dhcp	359
retransmit	725
revision (mst)	743
rmon alarm	1583
rmon collection history	1586
rmon event	1587
router ospf	1261
router rip	1385
router-id	1260, 1338
rule	275

S

script apply	1497
script delete	1498
script list	1499
script show	1499
script validate	1500
sdm prefer	1603
security	407
service	451
service dhcp	991
service dhcpv6	1006
service-acl input	292
service-policy	684
session-timeout	1448
set description	1726
sflow destination	1631
sflow polling	1633
sflow polling (Interface Mode)	1634
sflow sampling	1635

show flow sampling (Interface Mode)	1636
show aaa ias-users	260
show aaa servers	726
show aaa statistics	261
show accounting methods	728
show admin-profiles	276
show arp	965
show arp access-list	390
show authentication methods	262
show authorization methods	263
show auto-copy-sw	1431
show backup-config	1519
show banner	1728
show boot	1432
show bootvar	1520
show boot-version	1730
show captive-portal	1440
show captive-portal client status	1450
show captive-portal configuration	1461
show captive-portal configuration client status	1451
show captive-portal configuration interface	1462
show captive-portal configuration locales	1463
show captive-portal configuration status	1464
show captive-portal interface client status	1452
show captive-portal interface configuration status	1454
show captive-portal status	1441
show captive-portal user	1456
show checkpoint statistics	1730
show class-map	685
show classofservice dot1p-mapping	687
show classofservice ip-dscp-mapping	689
show classofservice traffic-class-group	908
show classofservice trust	692
show cli modes	277
show clock	1494
show copper-ports tdr	1579
show crypto certificate mycertificate	1811
show crypto key mypubkey	1680
show crypto key pubkey-chain ssh	1681

show cut-through mode	1731
show debugging	1629
show dhcp l2relay agent-option vlan	350
show dhcp l2relay all	346
show dhcp l2relay circuit-id vlan	352
show dhcp l2relay interface	347
show dhcp l2relay remote-id vlan	353
show dhcp l2relay stats interface	348
show dhcp l2relay subscription interface	349
show dhcp l2relay vlan	351
show dhcp lease	361
show diffserv	693
show diffserv service brief	696
show diffserv service interface	694
show diffserv service interface port-channel	695
show dos-control	1537
show dot1x	862
show dot1x advanced	877
show dot1x authentication-history	864
show dot1x clients	866
show dot1x interface	869
show dot1x interface statistics	871
show dot1x users	873
show dvlan-tunnel	805
show dvlan-tunnel interface	806
show ethernet cfm domain	461
show ethernet cfm errors	460
show ethernet cfm maintenance-points local	462
show ethernet cfm maintenance-points remote	463
show ethernet cfm statistics	464
show fiber-ports optical-transceiver	1580
show fip-snooping	919
show fip-snooping enode	921
show fip-snooping fcf	923
show fip-snooping sessions	926
show fip-snooping statistics	934
show fip-snooping vlan	941
show gvrp configuration	481
show gvrp error-statistics	482

show gvrp statistics	483
show hardware profile	1732
show hosts	523
show interfaces advanced firmware	1733
show interfaces advertise	422
show interfaces configuration	424
show interfaces cos-queue	696
show interfaces counters	425
show interfaces description	429
show interfaces detail	430
show interfaces loopback	1152
show interfaces media-type	1734
show interfaces port-channel	631
show interfaces priority-flow-control	949
show interfaces random-detect	699
show interfaces status	433
show interfaces switchport	807
show interfaces traffic-class-group	909
show interfaces tunnel	1392
show ip access-lists	294
show ip address-conflict	524
show ip arp inspection	391
show ip arp inspection vlan	394
show ip brief	1078
show ip dhcp binding	993
show ip dhcp conflict	994
show ip dhcp global configuration	994
show ip dhcp pool	995
show ip dhcp relay	1065
show ip dhcp server statistics	996
show ip dhcp snooping	374
show ip dhcp snooping binding	376
show ip dhcp snooping database	377
show ip dhcp snooping interfaces	377
show ip dhcp snooping statistics	379
show ip dvmrp	1021
show ip dvmrp interface	1022
show ip dvmrp neighbor	1022
show ip dvmrp nexthop	1023

show ip dvmrp prune	1024
show ip dvmrp route	1025
show ip helper statistics	1066
show ip helper-address	525, 1064
show ip http server secure status	1812
show ip http server status	1812
show ip igmp	1035
show ip igmp groups	1036
show ip igmp interface	1038
show ip igmp interface stats	1040
show ip igmp membership	1039
show ip igmp snooping	490
show ip igmp snooping groups	491
show ip igmp snooping interface	492
show ip igmp snooping mrouter	493
show ip igmp snooping querier	504
show ip igmp-proxy	1046
show ip igmp-proxy groups	1048
show ip igmp-proxy groups detail	1049
show ip igmp-proxy interface	1047
show ip interface	1079
show ip irdp	1372
show ip mcast boundary	1172
show ip mcast mroute	1173
show ip mcast mroute group	1174
show ip mcast mroute source	1175
show ip mcast mroute static	1176
show ip multicast	1171
show ip multicast interface	1172
show ip ospf	1261
show ip ospf abr	1269
show ip ospf area	1270
show ip ospf asbr	1273
show ip ospf database	1274
show ip ospf database database-summary	1277
show ip ospf interface	1279
show ip ospf interface brief	1281
show ip ospf interface stats	1283
show ip ospf neighbor	1284

show ip ospf range	1287
show ip ospf statistics	1289
show ip ospf stub table	1291
show ip ospf traffic	1292
show ip ospf virtual-link	1294
show ip ospf virtual-links brief	1296
show ip pim bsr-router	1177
show ip pim interface	1178
show ip pim neighbor	1180
show ip pim rp hash	1181
show ip pim rp mapping	1182
show ip protocols	1082
show ip rip	1386
show ip rip interface	1387
show ip rip interface brief	1388
show ip route	1087
show ip route configured	1089
show ip route connected	1090
show ip route preferences	1091
show ip route summary	1092
show ip source binding	561
show ip ssh	1682
show ip telnet	1781
show ip traffic	1093
show ip verify interface	559
show ip verify source interface	560
show ip vlan	1095
show ip vrrp interface	1420
show ipv6 access-lists	535
show ipv6 brief	1123
show ipv6 dhcp	1007
show ipv6 dhcp binding	1007
show ipv6 dhcp interface (Privileged EXEC)	1010
show ipv6 dhcp interface (User EXEC)	1008
show ipv6 dhcp interface out-of-band statistics	526
show ipv6 dhcp pool	1016
show ipv6 dhcp statistics	1016
show ipv6 interface	1124
show ipv6 interface management statistics	1127

show ipv6 interface out-of-band	528
show ipv6 mld groups	1128
show ipv6 mld interface	1131
show ipv6 mld snooping	545
show ipv6 mld snooping groups	547
show ipv6 mld snooping querier	554
show ipv6 mld traffic	1140
show ipv6 mld-proxy	1134
show ipv6 mld-proxy groups	1135
show ipv6 mld-proxy groups detail	1137
show ipv6 mld-proxy interface	1139
show ipv6 neighbors	1141
show ipv6 ospf	1338
show ipv6 ospf abr	1343
show ipv6 ospf area	1344
show ipv6 ospf asbr	1345
show ipv6 ospf border-routers	1346
show ipv6 ospf database	1346
show ipv6 ospf database database-summary	1351
show ipv6 ospf interface	1352
show ipv6 ospf interface brief	1353
show ipv6 ospf interface stats	1354
show ipv6 ospf interface vlan	1356
show ipv6 ospf neighbor	1357
show ipv6 ospf range	1359
show ipv6 ospf stub table	1360
show ipv6 ospf virtual-link brief	1362
show ipv6 ospf virtual-links	1361
show ipv6 pim	1196
show ipv6 pim bsr	1198
show ipv6 pim interface	1200
show ipv6 pim neighbor	1201
show ipv6 pim rp mapping	1202
show ipv6 pim rphash	1202
show ipv6 route	1142
show ipv6 route preferences	1144
show ipv6 route summary	1145
show ipv6 traffic	1146
show ipv6 vlan	1149

show iscsi	570
show iscsi sessions	571
show isdp	333
show isdp entry	334
show isdp interface	336
show isdp neighbors	337
show isdp traffic	339
show lacp	633
show line	1542
show link-dependency	580
show lldp	591
show lldp dcbx	895
show lldp interface	592
show lldp local-device	593
show lldp remote-device	595
show lldp statistics	597
show lldp tlv-select	894
show logging	1703
show logging email statistics	406
show logging file	1704
show mac access-list	295
show mac address-table	312
show mac address-table address	313
show mac address-table count	314
show mac address-table dynamic	315
show mac address-table filtering	311
show mac address-table interface	316
show mac address-table multicast	310
show mac address-table static	318
show mac address-table vlan	319
show mail-server	411
show management access-class	1551
show management access-list	1552
show memory cpu	1735
show monitor session	641
show mvr	610
show mvr interface	613
show mvr members	612
show mvr traffic	615

show nsf	1736
show parser macro	1476
show passwords configuration	1574
show passwords result	1576
show policy-map	700
show policy-map interface	701
show port protocol	811
show ports security	320
show ports security addresses	321
show power-usage-history	1737
show process cpu	1738
show radius statistics	729
show rmon alarm	1588
show rmon alarms	1590
show rmon collection history	1591
show rmon events	1592
show rmon history	1594
show rmon log	1597
show rmon statistics	1598
show routing heap summary	1297
show running-config	1521
show sdm prefer	1605
show service-acl interface	293
show service-policy	702
show sessions	1742
show sflow agent	1637
show sflow destination	1638
show sflow polling	1639
show sflow sampling	1640
show slot	1743
show snmp	1643
show snmp engineID	1645
show snmp filters	1646
show snmp group	1647
show snmp user	1649
show snmp views	1651
show snmp configuration	1480
show snmp server	1481
show snmp status	1483

show spanning-tree	744
show spanning-tree summary	751
show startup-config	1522
show statistics	434
show statistics port-channel	635
show statistics switchport	438
show storm-control	440
show supported cardtype	1744
show supported switchtype	1745
show switch	1747
show switchport protected	448
show switchport voice	324
show syslog-servers	1705
show system	1757
show system fan	1757
show system id	1758
show system power	1759
show system temperature	1760
show tacacs	776
show tech-support	1762
show time-range	1789
show trapflags	1652
show udd	788
show users	1765
show users accounts	265
show users login-history	266
show version	1766
show vlan	812
show vlan association mac	814
show vlan association subnet	815
show vlan private-vlan	836
show voice vlan	842
show vrrp	1412
show vrrp interface	1415
show vrrp interface brief	1417
show vrrp interface stats	1418
shutdown	441
slot	1727
snmp-server community	1654

snmp-server community-group	1656
snmp-server contact	1657
snmp-server enable traps	1657
snmp-server engineID local	1660
snmp-server filter	1661
snmp-server group	1663
snmp-server host	1664
snmp-server location	1666
snmp-server user	1667
snmp-server v3-host	1670
snmp-server view	1668
sntp	992
sntp authenticate	1484
sntp authentication-key	1485
sntp broadcast client enable	1486
sntp client poll timer	1487
sntp server	1487
sntp trusted-key	1488
sntp unicast client enable	1489
source-ip	733
spanning-tree	752
spanning-tree auto-portfast	753
spanning-tree bpdu flooding	754
spanning-tree bpdu-protection	754
spanning-tree cost	755
spanning-tree disable	756
spanning-tree forward-time	757
spanning-tree guard	758
spanning-tree loopguard	759
spanning-tree max-age	760
spanning-tree max-hops	760
spanning-tree mode	761
spanning-tree mst configuration	762
spanning-tree mst cost	763
spanning-tree mst port-priority	764
spanning-tree mst priority	765
spanning-tree portfast	766
spanning-tree portfast bpdufilter default	767
spanning-tree portfast default	767

spanning-tree port-priority	768
spanning-tree priority	769
spanning-tree tenguard	770
spanning-tree transmit hold-count	771
speed	441, 1544
split-horizon	1389
stack	1767
stack-port	1768
standby	1769
state	1814
storm-control broadcast	443
storm-control multicast	444
storm-control unicast	445
switch renumber	1770
switchport access vlan	816
switchport forbidden vlan	817
switchport general acceptable-frame-type tagged-only	818
switchport general allowed vlan	818
switchport general ingress-filtering disable	819
switchport general pvid	820
switchport mode	821
switchport mode private-vlan	833
switchport private-vlan	832
switchport protected	446
switchport protected name	447
switchport trunk	822
switchport voice detect auto	327

T

tacacs-server host	777
tacacs-server key	778
tacacs-server timeout	779
telnet	1770
terminal length	1783
terminal monitor	1706
test copper-port tdr	1581
timeout	734, 779
time-range	1785
timers pacing flood	1298
timers pacing lsa-group	1299

timers spf	1300
traceroute	1773
traceroute ethernet cfm	458
traceroute ipv6	1149
traffic-class-group max-bandwidth	902
traffic-class-group min-bandwidth	904
traffic-class-group strict	905
traffic-class-group weight	907
traffic-shape	703
tunnel destination	1393
tunnel mode ipv6ip	1394
tunnel source	1395
U	
udld enable (Global Config)	783
udld enable (Interface Config)	786
udld message time	785
udld port	787
udld reset	784
udld timeout interval	785
update bootcode	1524
usage	735
user group	1457, 1466
user group moveusers	1466
user group name	1467
user name	1459
user password	1460
user session-timeout	1460
user-key	1683
user-logout	1458
username	267
username (Mail Server Configuration Mode)	409
username unlock	270
V	
verification	1449
vlan	824
vlan (Global Config)	825
vlan association mac	826
vlan association subnet	826

vlan database	827
vlan makestatic	828
vlan protocol group	829
vlan protocol group add protocol	830
vlan protocol group name	831
vlan protocol group remove	831
voice vlan	840
voice vlan (Interface)	840
voice vlan data priority	842
vrrp accept-mode	1400
vrrp authentication	1401
vrrp description	1402
vrrp ip	1403
vrrp mode	1405
vrrp preempt	1405
vrrp priority	1406
vrrp timers advertise	1407
vrrp timers learn	1408
vrrp track interface	1409
vrrp track ip route	1410
W	
write	1525



Printed in the U.S.A.

www.dell.com | support.dell.com