Commands Reference

BSG8ew 1.0 and BSG12ew/aw/tw 1.0

Business Services Gateway

Document Status: **Standard**

Document Number: **NN47928-100**

Document Version: **02.02**

Date: **September 2008**

NORTEL

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

New in this release. 23
Features 23
Layer 2 commands 23
Layer 3 commands 23
BSG commands 24
Wireless commands 24
How to get help 29
Getting Help from the Nortel Web site 29
Getting Help over the phone from a Nortel Solutions Center 29
Getting Help from a specialist by using an Express Routing Code 29
Getting Help through a Nortel distributor or reseller 30
Introduction 31
Logging on to the CLI 31
Command modes. 33
Layer 2 command modes 34
Command modes 34
Protocol-specific modes 35
Layer 3 command modes 37
Protocol Independent Multicast component mode 37
Router configuration mode 37
VRRP router configuration mode 37
VRRP interface configuration mode 37
Technical Report 69 mode 37
Hierarchy of command modes 38
Using command modes. 39
Privileged Exec mode 39
Global configuration mode 39
Interface configuration mode 40
Config-VLAN mode 41
Line configuration mode 42
Layer 2 commands. 43
Spanning Tree Protocol commands 44
clear spanning-tree counters 46
clear spanning-tree detected protocols 47
debug spanning-tree 48
instance 50
name 51

revision . . . 52
show spanning-tree bridge . . . 53
show spanning-tree—detail, active . . . 54
show spanning-tree interface . . . 55
show spanning-tree—summary, blockedports, pathcost . . . 56
show spanning-tree mst—CIST or specified mst Instance . . . 57
show spanning-tree mst configuration . . . 58
show spanning-tree mst—common internal spanning tree or specified mst instance 59
show spanning-tree mst—port-specific configuration . . . 60
show spanning-tree root . . . 61
shutdown spanning-tree . . . 62
spanning-tree . . . 63
spanning-tree priority . . . 64
spanning-tree compatibility . . . 65
spanning-tree mode . . . 66
spanning-tree auto-edge . . . 67
spanning-tree mst configuration . . . 68
spanning-tree mst hello-time . . . 69
spanning-tree mst max-hops . . . 70
spanning-tree pathcost dynamic . . . 71
spanning-tree path cost method . . . 72
spanning-tree - Properties of an interface . . . 73
spanning-tree mst - Properties of an interface for MSTP . . . 74
spanning-tree timers . . . 75
spanning-tree transmit hold-count . . . 76
Port based network access control commands . . . 77
aaa authentication dot1x default . . . 78
debug dot1x . . . 79
dot1x access-control . . . 80
dot1x control-direction . . . 81
dot1x default . . . 82
dot1x init-session . . . 83
dot1x init-session-reauth . . . 84
dot1x auth-mode . . . 85
dot1x local-database . . . 86
dot1x max-req . . . 87
dot1x max-start . . . 88
dot1x port-control . . . 89
dot1x re-authenticate . . . 90
dot1x reauthentication . . . 91
dot1x system-auth-control . . . 92
dot1x timeout . . . 93

set nas-id 95
show dot1x 96
shutdown dot1x 97
Remote Authentication Dial-in User Service commands 98
debug radius 99
radius-server host 100
show radius server 101
show radius statistics 102
TACACS commands 103
debug tacacs 104
show tacacs 105
tacacs-server host 106
tacacs-server retransmit 107
tacacs use-server address 108
Internet Group Management Protocol snooping commands 109
debug ip igmp snooping 110
ip igmp snooping 111
ip igmp snooping fast-leave 112
ip igmp snooping group-query-interval 113
ip igmp snooping mrouter 114
ip igmp snooping mrouter-time-out 115
ip igmp snooping port-purge-interval 116
ip igmp snooping proxy-reporting 117
ip igmp snooping querier 118
ip igmp snooping query-interval 119
ip igmp snooping report-forward 120
ip igmp snooping report-suppression-interval 121
ip igmp snooping retry-count 122
ip igmp snooping version 123
show ip igmp snooping 124
show ip igmp snooping forwarding-database 125
show ip igmp snooping globals 126
show ip igmp snooping groups 127
show ip igmp snooping mrouter 128
show ip igmp snooping statistics 129
shutdown snooping 130
snooping multicast-forwarding-mode 131
Syslog commands 132
clear logs 133
cmdbuffs 134
logging 135
mailserver 137

receiver mail-id . . . 138
sender mail-id . . . 139
show email alerts . . . 140
show logging . . . 141
Secure Shell commands . . . 142
debug ssh . . . 143
ip ssh . . . 144
show ip ssh . . . 145
Secure Sockets Layer commands . . . 146
debug ssl . . . 147
ip http secure . . . 148
show ip http secure server status . . . 149
show ssl server-cert . . . 150
ssl gen cert-req algo rsa sn . . . 151
ssl server-cert . . . 152
System feature commands . . . 153
archive download-sw . . . 155
archive select . . . 156
authorized-manager ip-source . . . 157
base-mac . . . 159
cli console . . . 160
clock set . . . 161
copy . . . 162
copy-file . . . 163
copy logs . . . 164
copy startup-config . . . 165
debug-logging . . . 166
default ip address allocation protocol . . . 167
default management port ip address . . . 168
default mode . . . 169
default restore-file . . . 170
default tr69 . . . 171
default vlan mgmt port ip address . . . 172
disable login . . . 173
dump network status . . . 174
enable login . . . 175
erase . . . 176
flowcontrol . . . 177
jumbo frame support . . . 178
interface . . . 179
ip address . . . 181
ip address—DHCP, RARP . . . 182

ip address negotiated . . . 183
ip http port . . . 184
login authentication . . . 185
mac-address . . . 186
mtu frame size . . . 187
network-type wan . . . 188
private link . . . 189
prompt . . . 190
set bootdelay . . . 191
set ip http . . . 192
show authorized-managers . . . 193
show clock . . . 194
show debugging . . . 195
show debug-logging . . . 196
show files . . . 197
show flow-control . . . 198
show http server status . . . 199
show ip interface . . . 200
show interface mtu . . . 201
show interfaces . . . 202
show interfaces—counters . . . 204
show management vlan . . . 205
show nvram . . . 206
show running config . . . 207
show sub-system information . . . 208
show system information . . . 209
show tasks . . . 210
show uplink rate-limit status . . . 211
shutdown—physical/VLAN/port-channel/tunnel/PPP Interface . . . 212
snmp trap link-status . . . 213
switch name . . . 214
switchport . . . 215
system set factory default . . . 216
tunnel checksum . . . 217
tunnel mode . . . 218
tunnel path-mtu-discovery . . . 219
tunnel udlr . . . 220
uplink rate limit . . . 221
uplink rate limit enable / disable . . . 222
write . . . 223
Power over Ethernet commands . . . 224
power inline . . . 225

power inline priority . . . 226
set poe . . . 227
show power detail . . . 228
show power inline . . . 229
System commands . . . 230
alias . . . 231
clear screen . . . 232
close line vty . . . 233
configure terminal . . . 234
disable . . . 235
enable . . . 236
enable password . . . 237
end . . . 238
exec-timeout . . . 239
exit . . . 240
group . . . 241
help . . . 242
line . . . 243
line configuration mode . . . 244
listgroups . . . 245
listuser . . . 246
lock . . . 247
logout . . . 248
moduser . . . 249
pagination . . . 250
password . . . 251
run script . . . 252
show aliases . . . 253
show history . . . 254
show line . . . 255
show privilege . . . 256
show users . . . 257
username . . . 258
RMON commands . . . 259
rmon alarm . . . 260
rmon collection history . . . 262
rmon collection stats . . . 263
rmon event . . . 264
set rmon . . . 265
show rmon . . . 266
Virtual local area network commands . . . 267
debug vlan . . . 269

group restricted . . . 271
mac-address-table aging-time . . . 272
mac-address-table static multicast . . . 273
mac-address-table static unicast . . . 275
map protocol . . . 276
port protocol-vlan . . . 277
ports . . . 278
protocol-vlan . . . 279
set garp timer . . . 280
set gmrp . . . 281
set gvrp . . . 282
set port gmrp . . . 283
set port gvrp . . . 284
show garp timer . . . 285
show mac-address-table . . . 286
show mac-address-table aging-time . . . 287
show mac-address-table count . . . 288
show mac-address-table dynamic multicast . . . 289
show mac-address-table dynamic unicast . . . 290
show mac-address-table static multicast . . . 291
show mac-address-table static unicast . . . 292
show protocol-vlan . . . 293
show vlan . . . 294
show vlan device capabilities . . . 295
show vlan device info . . . 296
show vlan port config . . . 297
show vlan protocols-group . . . 298
shutdown garp . . . 299
switchport acceptable-frame-type . . . 300
switchport ingress-filter . . . 301
switchport map protocols-group . . . 302
switchport mode . . . 303
switchport priority default . . . 304
switchport pvid . . . 305
vlan . . . 306
vlan map-priority . . . 307
vlan restricted . . . 308
Dynamic host configuration protocol commands . . . 309
DHCP client commands . . . 311
debug ip dhcp client . . . 311
ip address . . . 312
release . . . 313

renew . . . 314
show ip dhcp client stats . . . 315
DHCP relay commands . . . 316
debug ip dhcp relay . . . 316
ip dhcp relay . . . 317
ip dhcp relay information option . . . 318
ip dhcp server . . . 319
service dhcp-relay . . . 320
show dhcp-server . . . 321
show ip dhcp relay information . . . 322
show ip dhcp relay interface . . . 323
DHCP server commands . . . 324
debug ip dhcp server . . . 324
default-router . . . 325
dns-server . . . 326
domain-name . . . 327
excluded-address . . . 328
host hardware-type . . . 329
ip dhcp . . . 330
ip dhcp bootfile . . . 331
ip dhcp device . . . 332
ip dhcp next-server . . . 333
ip dhcp option . . . 334
ip dhcp pool . . . 335
lease . . . 336
netbios-name-server . . . 337
netbios-node-type . . . 338
network . . . 339
option . . . 340
service dhcp-server . . . 341
show ip dhcp server binding . . . 342
show ip dhcp server devices . . . 343
show ip dhcp server information . . . 344
show ip dhcp server pools . . . 345
show ip dhcp server statistics . . . 346
show snmp-server traps . . . 347
utilization threshold . . . 348
Simple Network Management Protocol version 3 commands . . . 349
show snmp . . . 351
show snmp agent information . . . 352
show snmp community . . . 353
show snmp engineID . . . 354

show snmp group . . . 355
show snmp group access . . . 356
show snmp inform statistics . . . 357
show snmp notif . . . 358
show snmp-server traps . . . 359
show snmp targetaddr . . . 360
show snmp targetparam . . . 361
show snmp user . . . 362
show snmp viewtree . . . 363
snmp agent status . . . 364
snmp allowed version . . . 365
snmp access . . . 366
snmp community index . . . 368
snmp engineid . . . 370
snmp group . . . 371
snmp notify . . . 372
snmp-server enable traps snmp authentication . . . 373
snmp targetaddr . . . 374
snmp targetparams . . . 376
snmp user . . . 378
snmp view . . . 379
snmp-server enable traps . . . 380
system contact . . . 381
system location . . . 382

Layer 3 commands. . . . 383

Internet Protocol commands . . . 384
arp timeout . . . 386
arp—IP address . . . 387
ip aggregate-route . . . 388
ip arp max-retries . . . 389
ip default-ttl . . . 390
ip directed-broadcast . . . 391
ip echo-reply . . . 392
ip mask-reply . . . 393
ip path mtu . . . 394
ip path mtu discover . . . 395
ip rarp client . . . 396
ip rarp client request . . . 397
ip redirects . . . 398
ip route . . . 399
ip routing . . . 400
ip unreachables . . . 401

maximum-paths 402
ping 403
show ip arp 404
show ip information 405
show ip pmtu 406
show ip rarp 407
show ip traffic 408
show ip route 409
traffic-share 410
Internet Group Management Protocol commands 411
debug ip igmp 412
ip igmp immediate-leave 413
ip igmp last-member-query-interval 414
ip igmp query-interval 415
ip igmp query-max-response-time 416
ip igmp robustness 417
ip igmp static-group 418
ip igmp version 419
no ip igmp 420
set ip igmp 421
show ip igmp global-config 422
show ip igmp groups 423
show ip igmp interface 424
show ip igmp sources 425
show ip igmp statistics 426
Route redistribution commands 427
as-num 428
default redistribute-policy 429
export ospf 430
redistribute-policy 431
router-id 432
show ip protocols 433
show redistribute information 434
show redistribute-policy 435
Virtual router redundancy protocol commands 436
debug VRRP 437
interface vlan 438
router vrrp 439
show vrrp —vrid 440
show vrrp interface vlan 441
vrrp-interval 442
vrrp-ip address 443

vrrp—preempt 444
vrrp—priority 445
vrrp - text-authentication 446
Routing Information Protocol commands 447
auto-summary 448
debug ip rip 449
default-metric 450
ip rip authentication mode 451
ip rip default route originate 452
ip rip receive version 453
ip rip retransmission 454
ip rip security 455
ip rip send version 456
ip rip summary-address 457
ip spilt-horizon 458
neighbor 459
network 460
output-delay 461
passive-interface vlan 462
redistribute 463
router rip 464
show ip rip 465
timers basic 466
Open Shortest Path First commands 467
abr-type 469
area—default cost 470
area—nssa 471
area—range 472
area—stability-interval 474
area—stub 475
area—translation-role 476
area—virtual-link 477
ASBR Router 479
compatible rfc1583 480
debug ip ospf 481
default-information originate always 482
ip ospf authentication 483
ip ospf authentication-key 484
ip ospf cost 485
ip ospf dead-interval 486
ip ospf demand-circuit 487
ip ospf hello-interval 488

ip ospf message-digest-key 489
ip ospf network 490
ip ospf priority 491
ip ospf retransmit-interval 492
ip ospf transmit-delay 493
neighbor 494
network 495
passive-interface default 496
passive-interface vlan 497
redistribute 498
redist-config 499
router-id 500
router ospf 501
set nssa asbr-default-route translator 502
show ip ospf 503
show ip ospf border-routers 504
show ip ospf—database 505
show ip ospf—database summary 506
show ip ospf interface 507
show ip ospf neighbor 508
show ip ospf request-list 509
show ip ospf retransmission-list 510
show ip ospf route 511
show ip ospf—summary address 512
show ip ospf virtual-links 513
summary-address 514
Session Initiation Protocol commands 516
add dialplan 518
add sipserver MaximumSimWANCallsAllowed 519
add subscriber 520
bsg 521
CDR Mode 522
delete dialplan 523
delete sipserver MaximumSimWANCallsAllowed 524
delete subscriber 525
dialplan 526
domain 527
protocolheader 528
proxypolicy 529
registration 530
reload dialplan 531
set sipserver 532

set sipserver BackupModeGlobalDialPlanName 533
set sipserver—Brief / Detailed Traces 534
set sipserver CDRDirectoryPath 535
set sipserver CDRGeneration 536
set sipserver DNSLookupTimeOut 537
set sipserver domain name 538
set sipserver Dynamic Subscriber 539
set sipserver EnableSessionTimerRangeValidations 540
set sipserver ForkingPolicy 541
set sipserver –max/min/default timers 542
set sipserver - MaximumRegistrationPeriod 543
set sipserver MaximumSimWANCallsAllowed 544
set sipserver MinimumRegistrationPeriod 545
set sipserver NormalModeGlobalDialPlanName 546
set sipserver OrganizationHeader 547
set sipserver PolledServers 548
set sipserver ServerHeader 549
set sipserver SIP Message Dumps 550
set sipserver TFTPServerAddress 551
set sipserver - timer 552
show sipserver ActiveWANCallCount 554
show sipserver CDRDirectoryPath 555
show sipserver CDRGeneration 556
show sipserver dialplan 557
show sipserver DynamicSubscriber 558
show sipserver NormalModeGlobalDialPlanName 559
show sipserver OrganizationHeader 560
show sipserver - Port 561
show sipserver - Registration 562
show sipserver –scope bsg 563
show sipserver serverdomainname 564
show sipserver – Session Timer 565
show sipserver status 566
show sipserver subscriber details 567
show sipserver TFTPServerAddress 568
show sipserver - Timer 569
show sipserver - Traces 570
sip 571
sip – enable/disable 572
timer 573
trace sip 574
traces 575

transport . . . 576
update subscriber . . . 577
Linux tunnel commands . . . 578
clear dns—server cache . . . 579
copy . . . 580
copy ftp . . . 581
debug linuxtun . . . 582
dns-server forwarder . . . 583
dns-server forwarder – enable/disable . . . 584
dns-server forwarder zone . . . 585
set dns—server cache timeout . . . 586
show dns . . . 587
show tftp . . . 588
telnet . . . 589
tftp-server . . . 590
tftp-server topdir . . . 591
BSG commands . . . 593
Firewall commands . . . 594
access-list . . . 596
clear global statistics . . . 597
clear interface statistics . . . 598
commit . . . 599
disable . . . 600
dmz . . . 601
enable . . . 602
filter add . . . 603
firewall . . . 604
icmp . . . 605
icmp inspect . . . 606
ip filter fragments large . . . 607
ip inspect option . . . 608
ip inspect tcp enable . . . 609
ip inspect tcp half open . . . 610
ip inspect tcp syn wait . . . 611
ip verify reverse path . . . 612
netbios filtering . . . 613
no filter . . . 614
show firewall access-lists . . . 615
show firewall config . . . 616
show firewall dmz host . . . 617
show firewall filters . . . 618
show firewall half open connections . . . 619

show firewall interface config 620
show firewall interface statistics 621
show firewall logs 622
show firewall stateful table 623
show firewall stats 624
show url filters 625
trap threshold 626
untrusted port 627
url filter add 628
url filter delete 629
url filtering 630
Point-to-Point Protocol commands 631
debug ppp 632
keep-alive timeout 633
layer 634
multilink-group 635
peer 636
ppp authenticate username 637
ppp chap hostname 638
ppp username 639
uplink rate limit 640
Simple Network Time Protocol commands 641
clock summer-time recurring 642
show sntp clock 643
show sntp status 644
sntp 645
sntp authentication-key 646
sntp—enable/disable 647
sntp no time zone 648
sntp server 649
sntp set poll-interval 650
sntp time zone 651
Network Address Translation commands 652
debug nat 653
disable virtual server 654
enable virtual server 655
interface nat 656
ip nat 657
ip nat pool 658
ip nat—timeout 659
no virtual server 660
portrange 661

port trigger . . . 662
show ip nat . . . 663
show ip nat interface . . . 664
show nat config . . . 665
show portrange . . . 666
show port trigger . . . 667
show port trigger reserved list . . . 668
show virtual servers . . . 669
static nat . . . 670
virtual server . . . 671
Virtual private network policy commands . . . 672
access list . . . 673
clear vpn logs . . . 674
crypto ipsec mode . . . 675
crypto key mode . . . 676
crypto map . . . 677
crypto map - Interface . . . 678
crypto map ipsec . . . 679
ip ra-vpn pool . . . 680
isakmp peer identity . . . 681
isakmp policy encryption . . . 682
ra-vpn username . . . 683
set local identity . . . 684
set peer . . . 685
set session key . . . 686
set vpn . . . 687
show crypto map . . . 688
show ra-vpn users . . . 689
show ra-vpn address-pool . . . 690
show vpn config . . . 691
show vpn global statistics . . . 692
show vpn IKE statistics . . . 693
show vpn logs . . . 694
show vpn remote—ids . . . 695
vpn remote identity . . . 696
Diffserv commands . . . 697
class . . . 698
class-map . . . 699
no policy-map . . . 701
police . . . 702
policy-map . . . 703
queue threshold . . . 704

queue weight . . . 705
set qos . . . 706
set vlan traffic-classes . . . 707
show class-map . . . 708
show policer statistics . . . 709
show policy-map . . . 710
show qos default dhcp-dot1p mapping . . . 711
show qos status . . . 712
show queue stats . . . 713
show queuing . . . 714
show vlan port config . . . 715
show vlan traffic-classes . . . 716
shutdown qos . . . 717
switchport priority default . . . 718
vlan map—priority . . . 719
vlan max-traffic-class . . . 720
Access control list commands . . . 721
deny . . . 722
mac access-group . . . 724
mac access-list extended . . . 725
permit . . . 726
show access-lists . . . 728
VOIP commands . . . 729
reboot voip . . . 731
set country code . . . 732
set default codec type . . . 733
set default g723 encoding rate . . . 734
set default silent suppression . . . 735
set digital dial timeout . . . 736
set dtmf relay . . . 737
set dtmf rtp payload . . . 738
set fxo emergency-number . . . 739
set fxo forward phone-no . . . 740
set fxo hook detect time . . . 741
set fxo channel-number . . . 742
set fxo phone-number . . . 743
set fxo ring count . . . 744
set fxs call-forward . . . 745
set fxs call-forward number . . . 746
set fxs codec status . . . 747
set fxs codec type . . . 748
set fxs display-name . . . 749

set fxs fax-option . . . 750
set fxs line . . . 751
set fxs mailbox number . . . 752
set fxs mailbox password . . . 753
set fxs ring type . . . 754
set fxs user-number . . . 755
set fxs user-password . . . 756
set gmt-offset . . . 757
set ip tos . . . 758
set ip tos precedence option . . . 759
set mailbox ip . . . 760
set pstn-gateway . . . 761
set voice mailbox . . . 762
show voip codec config . . . 763
show voip config . . . 764
show voip firmware version . . . 765
show voip status . . . 766
shutdown . . . 767
voip1000 . . . 768
Technical Report 069 commands . . . 769
acs url . . . 770
connection request . . . 771
periodic inform . . . 772
periodic inform interval . . . 773
send inform . . . 774
show mgmt server config . . . 775
show tr69 status . . . 776
tr69 . . . 777
Wireless commands . . . 779
Wireless local area network commands . . . 780
config ap country . . . 782
config dot11—network . . . 783
config dot11 beaconperiod . . . 784
config dot11 channel . . . 785
config dot11 dtim . . . 786
config dot11 fragmentation . . . 787
config dot11 mode . . . 788
config dot11 preamble . . . 789
config dot11 profile clients . . . 790
config dot11 protection . . . 791
config dot11 rts-threshold . . . 792
config dot11 supported rates . . . 793

config dot11 turbo 794
config dot11 txpower 795
config dot11 wmm 796
config dot11 wmm-acknowledge-policy 797
config dot11 wmmparam 798
config macfilter 799
config wlan 800
config wlan broadcast-ssid 801
config wlan create 802
config wlan delete 803
config wlan interface 804
config wlan mac-filtering 805
config wlan pmksa timeout 806
config wlan security auth-type 807
config wlan security cipher-suite 808
config wlan security preauth 809
config wlan security pre-shared-key 810
config wlan security static-wep-key encryption 811
config wlan wep default-key 812
debug wlan 813
no wlan static-wep-key encryption 814
Variable definitions 814
show AP status 815
show client ap global 816
show dot11 817
show mac-filter-info 818
show wep default-key-info 819
show wlan 820
Digital Subscriber Line commands 821
dsl operating-mode 822
encapsulation 823
qos set 824
show dsl interface 825
show dsl interface pvc 826
show dsl traffic 827
traffic parameters set 828
vpi value 829
vci value 830
T1/E1 commands 831
cablelength long 832
cablelength short 833
channel-group 834

clear controller 835
clear controller statistics table 836
clock source 837
controller 838
controller mode 839
debug t1e1 840
dump t1e1 sib-counter 841
framing 842
linecode 843
line status change trap 844
loopback 845
mode 846
sendcode 847
show controllers 848
show controller statistics interval 849
show controller statistics table 850
show controllers t1e1 channel-groups 851
vendorid 852
Appendix A - Target based commands 853
negotiation 854
speed 855
duplex 856
mac-address-table aging-time 857
databits 858
parity 859
speed - console 860
stopbits 861

New in this release

This section details what is new in the *Commands Reference* guide for Business Services Gateway (BSG)8ew and BSG12ew/aw/tw 1.0.

Features

See the following sections for information about feature changes:

- Layer 2 commands (page 23)
- Layer 3 commands (page 23)
- BSG commands (page 24)
- Wireless commands (page 24)

Layer 2 commands

The following list provides the new layer 2 commands:

- Spanning Tree Protocol commands (page 24)
- Port based network access control commands (page 24)
- Remote authentication dial-in user service commands (page 24)
- Link aggregation commands (page 24)
- Syslog commands (page 25)
- Secure shell commands (page 25)
- Secure sockets layer commands (page 25)
- System feature commands (page 25)
- Power over Ethernet commands (page 25)
- System commands (page 25)
- Virtual local area network commands (page 25)
- Dynamic host configuration protocol commands (page 25)
- Simple network management protocol version 3 commands (page 26)

Layer 3 commands

The following list provides the new Layer 3 commands:

- Internet protocol commands (page 26)
- Internet group management protocol commands (page 26)
- Route redistribution commands (page 26)
- Virtual router redundancy protocol commands (page 26)
- Routing information protocol commands (page 26)
- Open shortest path first commands (page 26)

BSG commands

The following list provides the new Business Service Gateway (BSG) commands:

- Domain name server commands (page 26)
- Firewall commands (page 27)
- Point-to-point protocol commands (page 27)
- Simple network time protocol commands (page 27)
- Network address translation commands (page 27)
- Virtual private network policy commands (page 27)
- Remote access commands (page 27)

Wireless commands

The following list provides the new commands for Wireless CLI:

- Wireless local area network commands (page 27)
- Digital subscriber line commands (page 27)
- T1/E1 commands (page 27)

Spanning Tree Protocol commands

Spanning tree protocol (STP) is a link management protocol. For more information, see Spanning Tree Protocol commands (page 44).

Port based network access control commands

Port-based network access control (PNAC) is a portable implementation of the IEEE Std 802.1x PNAC. For more information, see Port based network access control commands (page 77).

Remote authentication dial-in user service commands

Remote authentication dial-in user service (RADIUS) is a client/server protocol and software. For more information, see Remote Authentication Dial-in User Service commands (page 98).

Link aggregation commands

Link aggregation is a method of combining physical network links into a single logical link for increased bandwidth.

Internet group management protocol snooping commands

Internet group management protocol (IGMP) is the protocol a host uses to inform a router when it joins (or leaves) an Internet multicast group. For more information, see Internet Group Management Protocol snooping commands (page 109).

Syslog commands

Syslog is a protocol used for capturing log information for devices on a network. For more information, see Syslog commands (page 132).

Secure shell commands

Secure shell (SSH) is a protocol for secure remote logon and other secure network services over an insecure network. For more information, see Secure Shell commands (page 142).

Secure sockets layer commands

Secure sockets layer (SSL) is a protocol developed for transmitting private documents through the Internet. For more information, see Secure Sockets Layer commands (page 146).

System feature commands

SMB BSG 8x12 offers a set of system features, such as logon services, copying or writing facilities, and duplex negotiation support. For more information, see System feature commands (page 153).

Power over Ethernet commands

Power over Ethernet (PoE) technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. For more information, see Power over Ethernet commands (page 224).

System commands

Use the system commands to manage access permissions, mode access, and terminal configurations on BSG. For more information, see System commands (page 230).

Virtual local area network commands

Virtual local area network (VLAN) is a group of devices on different physical LAN segments, which communicate with each other as if they were all on the same physical LAN segment. For more information, see Virtual local area network commands (page 267).

Dynamic host configuration protocol commands

Dynamic host configuration protocol (DHCP) allows dynamic configuration of a host computer. For more information, see Dynamic host configuration protocol commands (page 309).

Simple network management protocol version 3 commands

Simple network management protocol version 3 (SNMPv3) specifies a generic management framework, which is expandable for adding new management engines, security models, and access control models. For more information, see Simple Network Management Protocol version 3 commands (page 349).

Internet protocol commands

Internet protocol (IP) is an identifier for a computer or device on a transmission control protocol (TCP/IP) network. For more information, see Internet Protocol commands (page 384).

Internet group management protocol commands

Internet group management protocol (IGMP) reports group memberships to any immediate neighboring multicast router. For more information, see Internet Group Management Protocol commands (page 411).

Route redistribution commands

Route redistribution (RRD) allows different routing protocols to exchange routing information. For more information, see Route redistribution commands (page 427).

Virtual router redundancy protocol commands

Virtual router redundancy protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN. For more information, see Virtual router redundancy protocol commands (page 436).

Routing information protocol commands

Routing information protocol (RIP) is a protocol used for managing router information within a self-contained network. For more information, see Routing Information Protocol commands (page 447).

Open shortest path first commands

Open shortest path first (OSPF) protocol is an Interior Gateway Protocol (IGP) used for distributing routing information within a single autonomous system. For more information, see Open Shortest Path First commands (page 467).

Domain name server commands

Use domain name server (DNS) commands to configure the DNS.

Firewall commands

A firewall is a complete security solution. For more information, see Firewall commands (page 594).

Point-to-point protocol commands

The Point-to-point protocol (PPP) interface provides a point-to-point link between two communicating ends. For more information, see Point-to-Point Protocol commands (page 631).

Simple network time protocol commands

The simple network time protocol (SNTP) module synchronizes the time and date in BSG. For more information, see Simple Network Time Protocol commands (page 641).

Network address translation commands

Network address translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the internet, without requiring a registered subnet address. For more information, see Network Address Translation commands (page 652).

Virtual private network policy commands

Virtual private network (VPN) policy commands are used to authenticate the VPN. For more information, see Virtual private network policy commands (page 672).

Remote access commands

The remote access commands are used to configure remote access settings. For more information, see Diffserv commands (page 697).

Wireless local area network commands

The wireless local area network (WLAN) module controls the configuration of the wireless access point (AP) connected to the Business Service Gateway (BSG). For more information, see Wireless local area network commands (page 780).

Digital subscriber line commands

The digital subscriber line (DSL) module controls the configuration and control of the DSL modem connected to the BSG. For more information, see Digital Subscriber Line commands (page 821).

T1/E1 commands

T1/E1 is a digital WAN carrier facility. For more information, see T1/E1 commands (page 831).

How to get help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

The *Commands Reference* guide describes the Layer 2, Layer 3, Business Service Gateway (BSG), and wireless command line interface (CLI) commands.

Both the service providers and system administrators use the CLI commands. CLI is the interface to the software you use when you access the BSG. Install the BSG and configure it. If the installer does not have access to a network or a Web UI, they must configure the BSG using the CLI. You can access the CLI remotely through Telnet (with the Telnet server on the equipment). Use secure shell for secure CLI access.

With the CLI, you have more flexibility and control than with the Web user interface (UI). You can configure all of the available parameters in the CLI. But you cannot configure all the parameters in the Web UI. CLI is also faster than the GUI.

Navigation

- Command modes (page 33)
- Layer 2 commands (page 43)
- Layer 3 commands (page 383)
- BSG commands (page 593)
- Wireless commands (page 779)
- Appendix A - Target based commands (page 853)

Logging on to the CLI

Use the following procedure to log on to the CLI using Telnet or SSH.

Prerequisites

- Use the web GUI to enable Telnet.

Step	Action
1	Launch the Telnet or SSH application from your PC.
2	When prompted, enter the IP address of the BSG you want to access.
3	Enter your user name. First time users must enter nnadmin for the user name.
4	Enter your password. First time users must enter PlsChgme! for the password.
5	The BSG# or command prompt appears.

Command modes

This section describes the command modes available in the Small and Medium Business (SMB) Business Services Gateway (BSG) 8ew and BSG12ew/aw/tw 1.0.

Command modes navigation

- Layer 2 command modes(page 34)
- Layer 3 command modes(page 37)
- Hierarchy of command modes(page 38)

Layer 2 command modes

The following command modes are available in Layer 2:

- Command modes(page 34)
- Protocol-specific modes(page 35)

Command modes

Use Telnet or a Secure Shell (SSH) to access the command line interface (CLI). The following is a list of available modes when logon is complete:

- User EXEC mode(page 34)
- Privileged EXEC mode(page 34)
- Global configuration mode(page 34)
- Interface configuration mode (page 34)
- Protocol-specific modes (page 35)

User EXEC mode

After you log on to the device, you are automatically in the User EXEC mode. Use the User EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

Privileged EXEC mode

Privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case-sensitive. The Privileged EXEC mode prompt is the device name followed by the pound (#) sign.

Global configuration mode

Global configuration commands can be executed at any level of the system.

Interface configuration mode

Use interface configuration commands to modify specific interface operations. These commands always follow the global configuration command, which defines the interface type:

- Physical interface mode(page 35)
- Port channel interface mode(page 35)
- VLAN interface mode (page 35)
- Config VLAN mode(page 35)
- Tunnel interface mode(page 35)
- Out of band interface mode(page 35)
- PPP interface mode(page 35)

Physical interface mode

This is a sub-section of interface configuration mode. Use the physical interface mode to perform interface-specific operations. Use the `exit` command to return to the global configuration mode.

Port channel interface mode

Use the port channel interface mode to perform port-channel specific operations. Use the `exit` command to return to the global configuration mode.

VLAN interface mode

Use the VLAN interface mode to perform Layer 3 internet protocol/virtual local area network (L3-IPVLAN) specific operations. Use the `exit` command to return to the global configuration mode.

Config VLAN mode

Use this mode to configure VLAN properties.

Tunnel interface mode

Use the tunnel interface mode to perform tunnel-specific operations. Use the `exit` command to return to the global configuration mode.

Out of band interface mode

Use the out of band (OOB) interface mode to perform OOB-specific operations. Use `exit` to return to the global configuration mode.

PPP interface mode

Use the PPP interface mode to perform PPP-specific operations. Use `exit` to return to the global configuration mode

Protocol-specific modes

Use Telnet or a Secure Shell (SSH) to access the command line interface (CLI). The following is a list of available modes once logon is complete:

- MSTP configuration mode
- DiffSrv ClassMap configuration mode(page 36)
- DiffSrv Policy-Map configuration mode(page 36)
- DHCP pool configuration mode(page 36)
- ACL standard access list configuration mode(page 36)
- ACL MAC configuration mode(page 36)

MSTP configuration mode

Use this mode to configure the multiple spanning tree protocol (MSTP) specific parameters for the switch. Use the global configuration mode command `spanning-tree mst configuration` to enter the MSTP configuration mode. The prompt displayed at this mode is `is(config-mst)`.

Use the `exit` command to return to the global configuration mode.

DiffSrv ClassMap configuration mode

Use the Diff ClassMap configuration mode to create a class map for matching the packets to the class whose index is specified and to enter the class-map configuration mode. Use the global configuration mode command `class-map <short(1-65535)` to enter the DiffSvr ClassMap configuration mode. The prompt displayed at this mode is `iss(config-cmap)#.`

Use the `exit` command to return to the global configuration mode.

DiffSrv Policy-Map configuration mode

Use the DiffSrv Policy-Map configuration mode to create or modify a policy map. Use the global configuration mode command `policy-map <short(1-65535)>` to enter the DiffSvr Policy-Map configuration mode. The prompt displayed at this mode is `iss(config-pmap)#.`

Use the `exit` command to return to the global configuration mode.

DHCP pool configuration mode

Use this mode to configure the network pool/host configurations of a subnet pool.

Use the global configuration mode command `ip dhcp pool <integer(1-2147483647)>` to create a DHCP server address pool and place the user in the DHCP pool configuration mode. The prompt displayed at this mode is `iss(dhcp-config)#.`

Use the `exit` command to return to the global configuration mode.

ACL standard access list configuration mode

Standard access lists create filters based on IP address and network mask only (Layer 3 filters only).

Use the global configuration mode command `ip access-list standard <(1-1000)` to create IP access control lists (ACL) and enter the ACL standard access list configuration mode. The prompt displayed at this mode is `iss(config-std-nacl)#.`

Use the `exit` command to return to the global configuration mode.

ACL MAC configuration mode

Use the ACL MAC configuration mode to create Layer 2 MAC ACLs and return the ACL MAC configuration mode to the user.

Use the global configuration mode command `mac access-list extended <(1-65535)>` to enter the ACL MAC configuration mode. The prompt displayed at this mode is `iss(config-ext-macl)#.`

Use the `exit` command to return to the global configuration mode.

Layer 3 command modes

The following command modes are available in Layer 3.

- Protocol Independent Multicast component mode(page 37)
- Router configuration mode(page 37)
- VRRP router configuration mode(page 37)
- VRRP interface configuration mode(page 37)

Protocol Independent Multicast component mode

Use the Protocol Independent Multicast (PIM) component mode to configure the PIM component. Use the global configuration mode command `ip pim comp<componentid>` to enter the PIM component mode. Use the `exit` command to return to the global configuration mode.

Router configuration mode

Use the router configuration mode to configure the router protocol. Use the global configuration mode command `router <router protocol>` to enter the router configuration mode. The prompt displayed at this mode is `bsg(config-router)#.` Use the `exit` command to return to the global configuration mode or use the `end` command to exit to the Privileged EXEC mode.

VRRP router configuration mode

Use the VRRP router configuration mode to configure the virtual router. Use the global configuration mode command `router vrrp` to enter the virtual router redundancy protocol (VRRP) router configuration mode. Use the `exit` command to return to the global configuration mode or use the `end` command to exit to the Privileged EXEC mode.

VRRP interface configuration mode

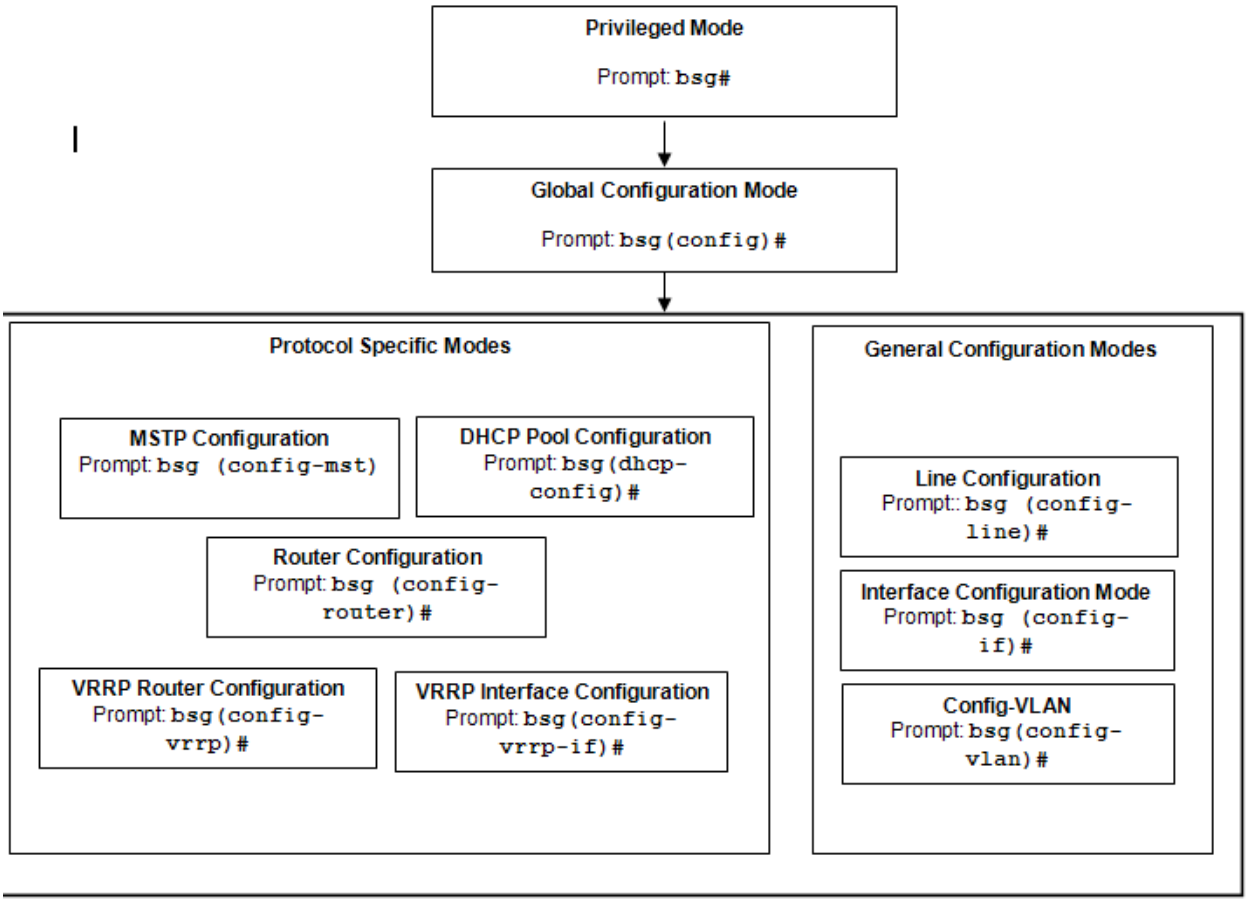
Use this mode to configure the VRRP interfaces. Use the global configuration mode command `interface Vlan <vlan id>` to enter the VRRP router configuration mode. The prompt displayed at this mode is `bsg(config-vrrp-if)#.` Use the `exit` command to return to the VRRP router configuration mode or use the `end` command to exit to the Privileged EXEC mode.

Technical Report 69 mode

Use this mode to configure Technical Report (TR) 69 related parameters. Use the tr69 command from the config mode. Use the `exit` command to return to the config mode and `end` command to exit to the Privileged EXEC mode.

Hierarchy of command modes

The following figures shows the hierarchy of command modes.



Using command modes

The Command Line Interface (CLI) uses different command modes, depending on the type of operation that you are performing. Each command listed in this reference guide includes information about which command mode to use for that specific command. This chapter describes how to access the command modes available on the CLI.

Each command mode has a specific prompt associated with it. The prompt indicates the current command mode:

- `bsg#` indicates Privileged Exec mode
- `bsg(config)#` indicates Global Configuration mode
- `bsg(config-if)#` indicates Interface Configuration mode
- `bsg(config-vlan)#` indicates Config-VLAN mode
- `bsg(config-line)#` indicates Line Configuration mode

Privileged Exec mode

Use the Privileged Exec mode to configure general operating parameters on the BSG system.

Using Privileged Exec mode

Procedure steps

Step	Action
1	Log on to the BSG system using Telnet or SSH.
2	The CLI defaults to Privileged Exec mode. *The prompt displayed for this mode is `BSG#`.*
3	At the prompt, enter a command.
4	To exit this mode, enter `logout`.

End

Global configuration mode

Use the Global Configuration mode to configure system-wide settings.

Using Global configuration mode

Procedure Steps

Step	Action

1. Log on to the BSG system using Telnet or SSH.
2. The CLI defaults to Privileged Exec mode.

   The prompt displayed for this mode is `BSG#`.
3. At the prompt, enter the following command: `configure terminal`.

   The system changes to Global Configuration mode, and displays the following prompt: `BSG(config)#`
4. At the prompt, enter a command.
5. Enter `exit` to return to the Privileged Exec mode.

End

Interface configuration mode

Use the Interface Configuration mode to configure specific interface settings.

Using Interface configuration mode

Procedure steps

Step	Action
1	Log on to the BSG system using Telnet or SSH.
2	The CLI defaults to Privileged Exec mode. *The prompt displayed for this mode is* `BSG#`.
3	At the prompt, enter the following command: `configure terminal`. *The system changes to Global Configuration mode, and displays the following prompt:* `BSG(config)#`
4	At the prompt, enter the following command: `interface <interface type> <interface id>` *The system changes to Interface Configuration mode, and displays the following prompt:* `BSG(config-if)#`
5	Enter `exit` to return to Global Configuration mode.
6	Enter `end` to return to the Privileged Exec mode.

End

Variable definitions

This table describes the variables used in the Interface Configuration mode.

Variable	Value
interface type	Specifies the interface type. The interface type can be a gigabitethernet or a fastethernet interface.
interface id	Specifies the physical interface ID including type, slot and port number. The value is numeric. Example: 0/2

Config-VLAN mode

Use the Config-VLAN mode to configure virtual LAN (VLAN) settings.

Using Config-VLAN mode

Procedure steps

Step	Action
1	Log on to the BSG system using Telnet or SSH.
2	The CLI defaults to Privileged Exec mode. *The prompt displayed for this mode is `BSG#`.*
3	At the prompt, enter the following command: `configure terminal`. *The system changes to Global Configuration mode, and displays the following prompt: `bsg(config)#`*
4	At the prompt, enter the following command: `vlan <vlan id>` *The system changes to Config-VLAN mode, and displays the following prompt: `bsg(config-vlan)#`*
5	Enter `exit` to return to Global Configuration mode.
6	Enter `end` to return to the Privileged Exec mode.

End

Variable Definitions

This table describes the variables used in the Config-VLAN mode.

Variable	Value
vlan id	Specifies the number that identifies the VLAN. The value is numeric. Example: 5.

Line configuration mode

Use the Line Configuration mode to configure terminal line settings.

Using Line configuration mode

Procedure steps

Step	Action
1	Log on to the BSG system using Telnet or SSH.
2	The CLI defaults to Privileged Exec mode. *The prompt displayed for this mode is* `bsg#`.
3	At the prompt, enter the following command: `configure terminal`. *The system changes to Global Configuration mode, and displays the following prompt:* `bsg(config)#`
4	At the prompt, enter the following command: `<vty>` *The system changes to Line Configuration mode, and displays the following prompt:* `bsg(config-line)#`
5	Enter `exit` to return to Global Configuration mode.
6	Enter `end` to return to the Privileged Exec mode.

End

Variable definitions

This table describes the variables used in the Line Configuration mode.

Variable	Value
console	Use when configuring lines that access the BSG through a console attached to the serial port.
vty	Use when configuring lines that access the BSG from a remote terminal using telnet or SSH.

Layer 2 commands

This section describes the commands used in configuring the Layer 2 Command Line Interface (CLI). The CLI supports a simple logon authentication mechanism. The authentication is based on a user name and password you provide during logon. The root user is factory-programmed with the password admin123.

Layer 2 commands navigation

- Spanning Tree Protocol commands (page 44)
- Port based network access control commands (page 77)
- Remote Authentication Dial-in User Service commands (page 98)
- TACACS commands (page 103)
- Internet Group Management Protocol snooping commands (page 109)
- Syslog commands (page 132)
- Secure Shell commands (page 142)
- Secure Sockets Layer commands (page 146)
- System feature commands (page 153)
- Power over Ethernet commands (page 224)
- RMON commands (page 259)
- Virtual local area network commands (page 267)
- Dynamic host configuration protocol commands (page 309)
- DHCP client commands (page 311)
- DHCP relay commands (page 316)
- DHCP server commands (page 324)
- Simple Network Management Protocol version 3 commands (page 349)

Spanning Tree Protocol commands

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all the switches in an extended network, forcing redundant paths into a standby or blocked state.

For proper functioning of an Ethernet network, only one active path must exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP can logically break such loops and prevent looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

STP navigation

- clear spanning-tree counters (page 46)
- clear spanning-tree detected protocols (page 47)
- debug spanning-tree (page 48)
- instance (page 50)
- name (page 51)
- revision (page 52)
- show spanning-tree bridge (page 53)
- show spanning-tree—detail, active (page 54)
- show spanning-tree interface (page 55)
- show spanning-tree—summary, blockedports, pathcost (page 56)
- show spanning-tree mst configuration (page 58)
- show spanning-tree mst—common internal spanning tree or specified mst instance (page 59)
- show spanning-tree mst—port-specific configuration (page 60)
- show spanning-tree root (page 61)
- shutdown spanning-tree (page 62)
- spanning-tree (page 63)
- spanning-tree priority (page 64)
- spanning-tree compatibility (page 65)
- spanning-tree mode (page 66)
- spanning-tree auto-edge (page 67)
- spanning-tree mst configuration (page 68)
- spanning-tree mst hello-time (page 69)
- spanning-tree mst max-hops (page 70)
- spanning-tree path cost method (page 72)
- spanning-tree - Properties of an interface (page 73)
- spanning-tree mst - Properties of an interface for MSTP (page 74)
- spanning-tree timers (page 75)

- spanning-tree transmit hold-count (page 76)

clear spanning-tree counters

Use this command to reset all bridge-level and port-level statistics counters.

Command mode

Global configuration

Syntax

```
clear spanning-tree counters
```

Related commands

`show spanning-tree interface`

`show spanning-tree mst configuration`

clear spanning-tree detected protocols

Use this command to restart the protocol migration process on all of the interfaces and force renegotiation with the neighboring switches.

Command mode

Privileged EXEC

Syntax

```
clear spanning-tree detected protocols [interface <interface-type>
<interface-id>]
```

Variable definitions

This table describes the variables used in the `instance` command.

Variable	Value
interface	Specifies the interface type and interface id.

Related commands

`show spanning-tree interface`

`show spanning-tree mst—port-specific configuration`

debug spanning-tree

Use this command to provide spanning tree debugging support. Precede this command with no to disable debugging.

Command mode

Privileged EXEC

Syntax

```
debug spanning-tree { all | errors |init-shut | management | memory |
bpdu | events | timer | state-machine { port-info | port-receive |
port-role-selection | role-transition | state-transition |
protocol-migration | topology-change | port-transmit | bridge-detection
} | redundancy | sem-variables}
```

```
no debug spanning-tree {all | errors | init-shut | management | memory |
bpdu | events | timer | state-machine {port-info | port-receive |
port-role-selection | role-transition | state-transition |
protocol-migration | topology-change | port-transmit | bridge-detection
} | redundancy | sem-variables}
```

Variable definitions

The following table describes the variables used in `debug spanning-tree` command.

Variable	Value
all	Specifies all RSTP and MSTP debug messages.
bpdu	Specifies BPDU-related messages.
bridge-detection	Specifies bridge detection messages.
errors	Specifies error code debug messages.
events	Specifies events-related messages.
init-shut	Specifies initialize and shutdown debug messages.
management	Specifies management messages.
Memory	Specifies memory-related messages.
port-info	Specifies port information messages.
port-receive	Specifies port-received messages.
port-role-selection	Specifies port role selection messages.
port-transmit	Specifies port transmission messages.
protocol-migration	Specifies protocol migration messages.
redundancy	Specifies redundancy-related messages.
role-transition	Specifies role transition messages.

Variable	Value
sem-variables	Specifies state-machine variables debug messages.
state machine	Specifies state-machine related debug messages.
state-transition	Specifies state transition messages.
timer	Specifies timer module messages.
topology-change	Specifies topology change messages.

Defaults

Debugging is disabled

Related commands

`show spanning-tree—summary, blockedports, pathcost`

instance

Use this command to map virtual local area networks (VLAN) to a multiple spanning tree (MST) instance. Precede this command with no to delete the instance and unmap specific VLANs from the MST instance. A single VLAN identified by VLAN ID number is specified by a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

Command mode

MSTP configuration

Syntax

```
instance <instance-id(1-64)> vlan <vlan-range>


no instance <instance-id(1-64)> [vlan <vlan-range>]
```

Variable definitions

This table describes the variables used in the `instance` command.

Variable	Value
instance-id(1-64)	Specifies spanning tree instances.
vlan-range	Specifies VLAN range associated with a spanning tree instance.

Defaults

VLANs mapped for instance 0: 1–1024, 1025–2048, 2049–3072, 3073–4094

Related commands

`show spanning-tree mst configuration`

name

Use this command to set the configuration name for the MST region. Precede this command with no to delete the configuration name. The name string is case sensitive.

Command mode

MSTP configuration

Syntax

```
name <string(optional max length)>
no name
```

Variable definitions

This table describes the variables used in the `name` command.

Variable	Value
string(optional max length)	Indicates maximum string length of 32 characters.

Defaults

The default configuration name is 00: 00: 00 :00: 00: 00:

Related commands

`show spanning-tree mst configuration`

revision

Use this command to set the configuration revision number for the MST region. Precede this command with no to delete the configuration revision number.

Command mode

MSTP configuration

Syntax

```
revision <value(0-65535)>


no revision
```

Variable definitions

This table describes the variables used in the `revision` command.

Variable	Value
<value(0-65535)>	Sets the configuration revision number.

Defaults

Configuration name is 0

Related commands

`show spanning-tree mst configuration`

show spanning-tree bridge

Use this command to display spanning tree information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show spanning-tree bridge [{address | forward-time | hello-time | id |
max-age | protocol | priority | detail }]
```

Variable definitions

This table describes the variables used in the `show spanning-tree bridge` command.

Variable	Value
address	Specifies bridge address.
detail	Displays bridge detail.
forward-time	Specifies bridge forward time.
hello-time	Specifies bridge hello time.
id	Specifies bridge ID.
max-age	Specifies bridge maximum age.
priority	Specifies bridge priority.
protocol	Specifies spanning tree protocol.

Related commands

`show spanning-tree—detail, active`

`spanning-tree mode`

`spanning-tree timers`

show spanning-tree—detail, active

Use this command to display spanning tree information.

Command mode

Privileged and User EXEC

Syntax

```
show spanning-tree {detail [active] | active [detail] }
```

Variable definitions

This table describes the variables used in the `show spanning-tree-detail, active` command.

Variable	Value
active	Displays the bridge and details of the active ports (active ports are those ports that are participating in the spanning tree).
detail	Displays details about the port and bridge. These include designated bridge details, designated port details, timer values, and root bridge.

Related commands

`show spanning-tree bridge`

`show spanning-tree interface`

`spanning-tree`

`spanning-tree priority`

`spanning-tree compatibility`

`spanning-tree mode`

`spanning-tree - Properties of an interface`

`spanning-tree mst - Properties of an interface for MSTP`

`spanning-tree timers`

`spanning-tree transmit hold-count`

show spanning-tree interface

Use this command to display spanning tree information.

Command mode

Privileged and User EXEC

Syntax

```
show spanning-tree interface <interface-type> <interface-id> [{cost | priority | portfast | rootcost | state | stats | detail}]
```

Variable definitions

This table describes the variables used in the `show spanning-tree interface` command.

Variable	Value
cost	Indicates spanning tree port cost.
detail	Displays details about the port and bridge.
portfast	Indicates spanning tree portfast state.
priority	Indicates spanning tree port priority.
rootcost	Indicates spanning tree rootcost (path cost to reach the root) value.
state	Indicates spanning tree state.
stats	Displays the input and output packets by switching path for the interface.

Related commands

`clear spanning-tree counters`

`clear spanning-tree detected protocols`

`show spanning-tree—detail, active`

`spanning-tree - Properties of an interface`

`spanning-tree mst - Properties of an interface for MSTP`

show spanning-tree—summary, blockedports, pathcost

Use this command to display spanning tree information. This command holds good for both RSTP and MSTP.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show spanning-tree [{summary | blockedports | pathcost method }]
```

Variable definitions

This table describes the variables used in the `show spanning-tree—summary, blockedports, pathcost` command.

Variable	Value
blockedports	Specifies blocked ports in the system.
pathcost method	Specifies pathcost method configured for a bridge.
summary	Displays summary of port states.

Defaults

Spanning tree is enabled with MSTP operating in the switch

Related commands

`show spanning-tree bridge`

`show spanning-tree interface`

`spanning-tree`

`spanning-tree priority`

`spanning-tree compatibility`

`spanning-tree mode`

`spanning-tree path cost method`

`spanning-tree - Properties of an interface`

`spanning-tree mst - Properties of an interface for MSTP`

`spanning-tree timers`

`spanning-tree transmit hold-count`

show spanning-tree mst—CIST or specified mst Instance

Use this command to display multiple spanning tree information for the Common Internal Spanning Tree (CIST) instance or specified MST instance. The MST option is available only when MSTP is the operational mode of the spanning tree.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show spanning-tree mst [<instance-id(1-64)>] [detail]
```

Variable definitions

This table describes the variables used in the `show spanning-tree mst—CIST` command.

Variable	Value
instance-id	Specifies the range of spanning tree instances.
detail	Specifies the spanning tree mst instance specific details.

Related commands

`instance`

`spanning-tree priority`

`spanning-tree mst - Properties of an interface for MSTP`

show spanning-tree mst configuration

Use this command to display multiple spanning tree instance configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show spanning-tree mst configuration
```

Related commands

instance

name

revision

show spanning-tree mst—common internal spanning tree or specified mst instance

Use this command to display multiple spanning tree information for the Common Internal Spanning Tree (CIST) instance or specified MST instance.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show spanning-tree mst [<instance-id(1-64)>] [detail]
```

Variable definitions

This table describes the variables used in the `show spanning-tree mst—common internal spanning tree or specified mst instance` command.

Variable	Value
detail	Specifies spanning tree MST instance-specific details.
instance-id	Specifies range of spanning tree instances.

Related commands

`instance`

`spanning-tree priority`

`spanning-tree mst - Properties of an interface for MSTP`

show spanning-tree mst—port-specific configuration

Use this command to display multiple spanning tree port-specific configuration.

Command mode

Privileged and User EXEC

Syntax

```
show spanning-tree mst [<instance-id(1-64)>] interface <interface-type>
<interface-id> [{stats | hello-time | detail }]
```

Variable definitions

This table describes the variables used in the `show spanning-tree mst—port-specific configuration command.`

Variable	Value
detail	Details multiple spanning tree port-specific configuration.
hello-time	Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.
instance-id	Specifies the range of spanning tree instances.
interface	Details interface type and interface id.
stats	Displays the input and output packets by switching path for the interface.

Related commands

`clear spanning-tree counters`

`clear spanning-tree detected protocols`

`instance`

`show spanning-tree interface`

`spanning-tree mst hello-time`

`spanning-tree mst - Properties of an interface for MSTP`

`spanning-tree - Properties of an interface`

show spanning-tree root

Use this command to display spanning tree information.

Command mode

Privileged and User EXEC

Syntax

```
show spanning-tree root [{address | cost | forward-time | hello-time | id
| max-age | port | priority | detail }]
```

Variable definitions

This table describes the variables used in the `show spanning-tree root command.`

Variable	Value
address	Specifies root bridge MAC address.
cost	Specifies cost value associated with the port.
detail	Displays details about the port and bridge. These include designated bridge details, designated port details, timer values, and root bridge.
forward-time	Specifies root bridge forward time
hello-time	Specifies root bridge hello time.
id	Specifies root bridge ID.
max-age	Specifies root bridge maximum age.
port	Specifies root port.
priority	Specifies root bridge priority.

Related commands

`show spanning-tree—summary, blockedports, pathcost`

`spanning-tree priority`

`spanning-tree timers`

shutdown spanning-tree

Use this command to shut down spanning tree operation. MSTP and RSTP are mutually exclusive and hence the MSTP module must be shutdown to start the RSTP module. The bridge module must be enabled to start RSTP.

Command mode

Global configuration

Syntax

```
shutdown spanning-tree
```

Defaults

MSTP is started and enabled

Related commands

`show spanning-tree—detail, active`

`spanning-tree mode`

spanning-tree

Use this command to enable the spanning tree operation. Precede this command with no to disable the spanning tree operation.

Command mode

Global configuration

Syntax

```
spanning-tree


no spanning-tree
```

Defaults

Spanning tree enabled is MSTP

Related commands

show spanning-tree—summary, blockedports, pathcost

spanning-tree priority

Use this command to set the bridge priority for the spanning tree in steps of 4096. Precede this command with no to set the bridge priority to the default value.

Command mode

Global configuration

Syntax

```
spanning-tree [mst <instance-id>] priority <value (0-61440)>


no spanning-tree [mst <instance-id>(1-64)> priority]
```

Variable definitions

This table describes the variables used in the `spanning-tree priority` command.

Variable	Value
mst <instance-id>	Specifies the range of spanning tree instances.
priority <value(0-61440)	Indicates switch priority value for the specified spanning-tree instance. Value ranges from 0 to 61440.

Defaults

32768

Related commands

`show spanning-tree—detail, active`

spanning-tree compatibility

Use this command to set the compatibility version for the spanning tree protocol. Precede this command with no to set the compatibility version for the spanning tree protocol to its default value.

Command mode

Global configuration

Syntax

```
spanning-tree compatibility {stp|rst|mst}


no spanning-tree compatibility
```

Variable definitions

This table describes the variables used in the `spanning-tree compatibility` command.

Variable	Value
`mst`	Specifies the MSTP configuration.
`rst`	Specifies the RSTP configuration.
`stp`	Specifies the STP configuration.

Defaults

If spanning tree enabled is `mst`, then the spanning tree is MSTP-compatible

If spanning tree enabled is `rst`, then the spanning tree is RSTP-compatible

Related commands

`show spanning-tree—detail, active`

spanning-tree mode

Use this command to set the spanning tree operating mode. When BSG boots up, spanning tree is enabled by default with MSTP operating in the switch.

Command mode

Global configuration

Syntax

```
spanning-tree mode {mst|rst}
```

Variable definitions

This table describes the variable used in the `spanning-tree mode` command.

Variable	Value
mst	Specifies the MSTP configuration mode.
rst	Specifies the RSTP configuration mode.

Defaults

MST

Related command

show spanning-tree—detail, active

spanning-tree auto-edge

Use this command to enable automatic detection of a bridge attached to an interface. Precede this command with no to disable automatic detection of a bridge attached to an interface.

Command mode

Interface configuration

Syntax

```
spanning-tree auto-edge
```

```
no spanning-tree auto-edge
```

Related commands

show spanning-tree bridge

spanning-tree mst configuration

Use this command to enter the MST configuration mode. In the MST mode, the switch supports up to 16 instances. This MST configuration submode is used to make instance-specific and MST region configurations only. The zeroth instance of MST is the common instance spanning tree which is created by default.

Command mode

Global configuration

Syntax

```
spanning-tree mst configuration
```

Related commands

`show spanning-tree mst configuration`

spanning-tree mst hello-time

Use this command to set the port-based hello timer value. Precede this command with no to set the port-based hello timer to the default value.

Command mode

Interface configuration

Syntax

```
spanning-tree mst hello-time <value(1-10)>


no spanning-tree mst hello-time
```

Defaults

Spanning-tree mst hello-time is 2 seconds

Related commands

`show spanning-tree bridge`

spanning-tree mst max-hops

Use this command to set the maximum number of hops permitted in the MST. Precede this command with no to set the maximum number of hops permitted in the MST to the default value. The root switch of the instance always sends a BPDU with a cost of 0 and the hop count set to the maximum value.

Command mode

Global configuration

Syntax

```
spanning-tree mst max-hops <value (6-40)>


no spanning-tree mst max-hops
```

Variable definitions

This table describes the variables used in the `spanning-tree mst max-hops` command.

Variable	Value
hop-count <1-10>	Specifies the number of hops in a region before the BDPU is discarded.

Defaults

20

Related commands

`show spanning-tree mst configuration`

spanning-tree pathcost dynamic

Use this command to set the maximum number of hops permitted in the MST. Precede this command with no to set the maximum number of hops permitted in the MST to the default value. The root switch of the instance always sends a BPDU with a cost of 0 and the hop count set to the maximum value.

Command mode

Global configuration

Syntax

```
spanning-tree pathcost dynamic


no spanning-tree pathcost dynamic
```

Defaults

disabled

Related commands

spanning-tree path cost method

spanning-tree compatibility

spanning-tree - Properties of an interface

spanning-tree mst - Properties of an interface for MSTP

spanning-tree path cost method

Use this command to set the method to calculate the port path cost. Precede this command with no to set the method to calculate the port value to its default value.

Command mode

Global configuration

Syntax

```
spanning-tree pathcost method{long|short}


no spanning-tree pathcost method
```

Variable definitions

This table describes the variables used in the `spanning-tree path cost method` command.

Variable	Value
long	Specifies 32-bit pathcost.
short	Specifies 16-bit pathcost.

Defaults

Long if MSTP or RSTP is running

Short if STP compatible with RSTP is running

Related commands

`show spanning-tree—summary, blockedports, pathcost`

spanning-tree - Properties of an interface

Use this command to set the spanning tree properties of an interface. Precede this command with no to set the spanning tree properties of an interface to the default value.

Command mode

Interface configuration

Syntax

```
spanning-tree {cost <value(1-200000000)> | disable | link-type
{point-to-point | shared } | portfast | port-priority <value(0-240)>}


no spanning-tree {cost | disable | link-type | portfast | port-priority}
```

Variable definitions

This table describes the variables used in the `spanning-tree - Properties of an interface` command.

Variable	Value
cost	Specifies the pathcost value associated with the port.
disable	Disables the spanning tree on the port.
link-type	Specifies the link type. The link is either a point-to-point link or a shared LAN segment where another bridge is present.
portfast	Specifies that the port only has hosts connected and transitions to forwarding rapidly.
port-priority	Specifies the port priority value.

Defaults

cost	2000000
link-type	shared
portfast	not in portfast mode
port-priority	128

Related commands

`show spanning-tree interface`

spanning-tree mst - Properties of an interface for MSTP

Use this command to set the spanning tree properties of an interface for MSTP. Precede this command with no to set the spanning tree properties of an interface for MSTP to the default value. If all interfaces have the same priority value, the MST puts the interface with the lowest interface number in the forwarding state and blocks other interfaces

Command mode

Interface configuration

Syntax

```
spanning-tree {cost
<value(1-200000000)>|disable|link-type{point-to-point|shared}|portfast|p
ort-priority <value(0-240)>}


no spanning-tree mst <instance-id(1-64)>{cost|port-priority | disable}
```

Variable definitions

This table describes the variables used in the `spanning-tree mst - Properties of an interface for MSTP` command.

Variable	Value
cost	Specifies the pathcost value associated with the port.
disable	Disables the spanning tree on the port.
instance-id(1-64)	Specifies the range of spanning tree instances.
port-priority	Specifies port priority value.

Defaults

cost	2000000
port-priority	128

Related commands

`show spanning-tree interface`

`show spanning-tree mst—port-specific configuration`

spanning-tree timers

Use this command to set the spanning tree timers. Precede this command with no to set the spanning tree timers to default values.

Command mode

Global configuration

Syntax

```
spanning-tree {forward-time <seconds(4-30) | hello-time <seconds(1-2) |
max-age <seconds(6-40)>}


no spanning-tree { forward-time | hello-time | max-age }
```

Variables definitions

This table describes the variables used in the `spanning-tree timers` command.

Variable	Value
forward-time <seconds(4-30)	Controls how fast a port changes its spanning tree state from blocking state to forwarding state.
hello-time <seconds(1-2)	Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.
max-age <seconds(6-40)	Specifies the maximum age allowed for the spanning tree protocol information learned from the network on any port before it is discarded.

Defaults

max-age	20 seconds
forward-time	15 seconds
hello-time	2 seconds

Related commands

`show spanning-tree bridge`

`show spanning-tree—detail, active`

spanning-tree transmit hold-count

Use this command to set the transmit hold-count value. Precede this command with no to set the transmit hold-count to the default value.

Command mode

Global configuration

Syntax

```
spanning-tree transmit hold-count <value (1-10)>


no spanning-tree transmit hold-count
```

Variable definitions

This table describes the variables used in the `spanning-tree transmit hold-count` command.

Variable	Value
transmit hold-count <value (1-10)>	Specifies the counter used to limit the maximum transmission rate of the switch.

Defaults

6

Related commands

`show spanning-tree—summary, blockedports, pathcost`

Port based network access control commands

Port based Network Access Control (PNAC) is a portable implementation of the IEEE Std 802.1x PNAC. It is used on both local area network (LAN) switches and wireless LAN access points to provide security services. When used in LAN switches, it offers access control to protected resources existing in the switched network. When used in WLAN access points, it provides authentication of the WLAN stations and improves the security by making use of the periodically exchanged key for encrypting data. PNAC can port to RTOS environments and interface to different switch hardware.

Port based network access control commands navigation

- aaa authentication dot1x default (page 78)
- debug dot1x (page 79)
- dot1x access-control (page 80)
- dot1x auth-mode (page 85)
- dot1x control-direction (page 81)
- dot1x default (page 82)
- dot1x init-session (page 83)
- dot1x init-session-reauth (page 84)
- dot1x local-database (page 86)
- dot1x max-req (page 87)
- dot1x max-start (page 88)
- dot1x port-control (page 89)
- dot1x re-authenticate (page 90)
- dot1x reauthentication (page 91)
- dot1x system-auth-control (page 92)
- dot1x timeout (page 93)
- set nas-id (page 95)
- show dot1x (page 96)
- shutdown dot1x (page 97)

aaa authentication dot1x default

Use this command to enable the dot1x local authentication or Remote Authentication Dial In User Service (RADIUS) server based remote authentication method for all ports.

Command mode

Global configuration

Syntax

```
aaa authentication dot1x default {group radius | local}
```

Variable definitions

This table describes the variables used in the `aaa authentication dot1x default` command.

Variable	Value
group radius	Specifies RADIUS server based authentication
local	Specifies local authentication.

Defaults

local

Related commands

`dot1x local-database`

`radius-server host`

`show dot1x`

debug dot1x

Use this command to enable debugging of the dot1x module. Precede this command with no to disable debugging of dot1x module.

Command mode

Privileged EXEC

Syntax

```
debug dot1x {all | errors | events | packets | state-machine |
redundancy}
```

```
no debug dot1x {all | errors | events | packets | state-machine |
redundancy}
```

Variable definitions

This table describes the variables used in the `debug dot1x` command.

Variable	Value
all	Specifies all dot1x debug messages.
errors	Specifies dot1x error code debug messages.
events	Specifies dot1x event debug messages.
packets	Specifies dot1x packet debug messages.
redundancy	Specifies redundancy related messages.
state-machine	Specifies state-machine related-event debug messages.

Defaults

Events debugging is enabled by default.

Related commands

`show dot1x`

dot1x access-control

Use this command to configure the supplicant access control. Precede this command with no to set the access control to inactive.

Command mode

Interface configuration

Syntax

```
dot1x access-control {active|inactive}


no dot1x access-control
```

Variable definitions

This table describes the variables used in the `dotx access-control` command.

Variable	Value
active	Set the port status as a combined port status of the authenticator and the supplicant.
inactive	Set the port status to the port status of the authenticator.

Defaults

Access control is inactive by default.

Related commands

`show dot1x`

dot1x control-direction

Use this command to configure port control direction. Precede this command with no to set the authenticator port control direction to both.

Command mode

Interface configuration

Syntax

```
dot1x control-direction {in|both}
```

```
no dot1x control-direction
```

Variable definitions

This table describes the variables used in the `dot1x control-direction` command.

Variable	Value
both	Specifies that authentication control is imposed on both incoming and outgoing packets.
in	Specifies that authentication control is imposed only on the incoming packets.

Defaults

Control direction is both by default.

Related commands

`show dot1x`

dot1x default

Use this command to configure dot1x with default values for this port.

Command mode

Interface configuration

Syntax

```
dot1x default
```

Defaults

Per-interface 802.1X protocol enable state	Enabled (force-authorized)
Periodic re authentication	Disabled
Number of seconds between re authentication attempts	3600 seconds
Quiet period	60 seconds
Retransmission time	30 seconds
Maximum retransmission number	2 times
Client timeout period	30 seconds
tx period	30 seconds
Authentication server timeout period	30 seconds

Related commands

`show dot1x`

dot1x init-session

Use this command to initiate dot1x authentication session.

Command mode

Global configuration mode

Syntax

```
dot1x init-session <supp addr - aa.aa.aa.aa.aa.aa>
```

Variable definitions

This table describes the variables used in the `dot1x init-session` command.

Variable	Value
supp addr - aa.aa.aa.aa.aa.aa	Specifies the supplicant address to initiate.

Related commands

`show dot1x`

dot1x init-session-reauth

Use this command to initiate the dot1x reauthentication session.

Command mode

Global configuration mode

Syntax

```
dot1x init session-reauth <supp addr - aa.aa.aa.aa.aa.aa>
```

Variable definitions

This table describes the variable used in the `dot1x init-session-reauth` command.

Variable	Value
supp addr - aa.aa.aa.aa.aa.aa	Specifies the supplicant address to initiate.

Related commands

`show dot1x`

dot1x auth-mode

Use this command to configure the port authentication mode. Precede this command with no to set the port authentication mode to port based.

Command mode

Interface configuration mode

Syntax

```
dot1x auth-mode {port-based | mac-based}


no dot1x auth-mode
```

Variable definitions

This table describes the variables used in the `dot1x auth-mode` command.

Variable	Value
port-based	Specifies the value to configure port-based authentication mode.
mac-based	Specifies the value to configure mac-based authentication mode.

Related commands

`show dot1x`

dot1x local-database

Use this command to configure the dot1x authentication server database with user name and password. Precede this command with no to delete an entry from the dot1x authentication server database.

Command mode

Global configuration

Syntax

```
dot1x local-database <username> password <password> permission {allow | deny} [<auth-timeout (value(1-7200))>] [interface <interface-type> <interface-list>]


no dot1x local-database username
```

Variable definitions

This table describes the variables used in the `dot1x local-database` command.

Variable	Value
auth-timeout	Specifies the number of seconds between authentication attempts.
interface	Specifies the port list of the interface on which dot1x authentication can be applied.
password	Specifies the password.
permission	Specifies whether the user is allowed or denied access on a set of ports.
username	Specifies user name.

Defaults

permission	allow
interface-list	all the physical interfaces

Related commands

`aaa authentication dot1x default`

`show dot1x`

dot1x max-req

Use this command to set the maximum number of Extensible Authentication Protocol (EAP) retries to the client before restarting authentication process. Precede this command with no to set the maximum number of EAP retries to the client to default value.

Command mode

Interface configuration

Syntax

```
dot1x max-req <count(1-10)>


no dot1x max-req
```

Variable definitions

This table describes the variables used in the `dot1x max-req` command.

Variable	Value
count(1-10)	Specifies number of EAP retries to the client.

Defaults

count	2

Related commands

`show dot1x`

dot1x max-start

Use this command to set the maximum number of EAP retries to the authenticator. Precede this command with no to set the maximum number of EAP retries to the authenticator to default value.

Command mode

Interface configuration

Syntax

```
dot1x max-start <count(1-10)>


no dot1x max-start
```

Variable definitions

This table describes the variables used in the `dot1x max-start` command.

Variable	Value
count(1-10)	Specifies the number of EAP retries to the authenticator. Value ranges from 1 to 10.

Defaults

count	3

dot1x port-control

Use this command to configure the authenticator port control parameter. Precede this command with no to set the authenticator port control state to force authorized.

Command mode

Interface configuration

Syntax

```
dot1x port-control {auto|force-authorized|force-unauthorized}
```

```
no dot1x port-control
```

Variable definitions

This table describes the variables used in the `dot1x port-control` command.

Variable	Value
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 server and the client.
force-authorized	All the traffic is allowed without any restrictions.
force-unauthorized	All the traffic over the interface will be blocked.

Defaults

Force-authorized is enabled

Related commands

`dot1x default`

`show dot1x`

dot1x re-authenticate

Use this command to initiate re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port.

Command mode

Privileged EXEC

Syntax

```
dot1x re-authenticate [interface <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `dot1x re-authenticate` command.

Variable	Value
interface	Specifies port number of the interface to re-authenticate.

Defaults

dot1x is enabled by default.

Related commands

`show dot1x`

dot1x reauthentication

Use this command to enable periodic re-authentication from authenticator to client. Precede this command with no to disable periodic re-authentication from authenticator to client.

Command mode

Interface configuration

Syntax

```
dot1x reauthentication
```

```
no dot1x reauthentication
```

Defaults

Periodic re-authentication is disabled

Related commands

dot1x default

dot1x timeout

show dot1x

dot1x system-auth-control

Use this command to enable dot1x in the switch. Precede this command with no to disable dot1x in the switch

Command mode

Global configuration

Syntax

```
dot1x system-auth-control


no dot1x system-auth-control
```

Defaults

dot1x is enabled

Related commands

show dot1x

shutdown dot1x

dot1x timeout

Use this command to set the dot1x timers. Precede this command with no to set the dot1x timers to the default values.

Command mode

Interface configuration

Syntax

```
dot1x timeout {quiet-period <value (0-65535)> | {reauth-period |
server-timeout | supp-timeout | tx-period | start-period | held-period |
auth-period }<value (1-65535)>}


no dot1x timeout {quiet-period | reauth-period | server-timeout |
supp-timeout | tx-period | start-period | held-period | auth-period}
```

Variable definitions

This table describes the variables used in the `dot1x timeout` command.

Variable	Value
auth-period	Specifies the number of seconds that the supplicant waits before timing-out the authenticator.
held-period	Specifies the number of seconds that the supplicant waits before trying to acquire the authenticator.
quiet-period	Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.
reauth-period	Specifies the number of seconds between re-authentication attempts.
server-timeout	Specifies the number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server.
start-period	Specifies the number of seconds that the supplicant waits between successive retries to the authenticator.
supp-timeout	Specifies the number of seconds that the switch waits for the retransmission of packets by the switch to the client.
tx-period	Specifies the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.

Defaults

quiet-period	60 seconds
reauth-period	3600 seconds
server-timeout	30 seconds
supp-timeout	30 seconds
tx-period	30 seconds
start-period	30 seconds
held-period	60 seconds
auth-period	30 seconds

Related commands

`dot1x default`

`dot1x max-req`

`dot1x reauthentication`

`show dot1x`

set nas-id

Use this command to set the dot1x network access server id.

Command mode

Global configuration

Syntax

```
set nas-id <identifier>
```

Variable definitions

This table describes the variables used in the `set nas-id` command.

Variable	Value
identifier	Specifies the dot1x network access server ID of string length 16.

Defaults

fsNas1

Related commands

`show dot1x`

show dot1x

Use this command to display dot1x information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dot1x [{interface <interface-type> <interface-id> | statistics
interface <interface-type> <interface-id> | supplicant-statistics
interface <interface-type> <interface-id>|local-database | mac-info
[address <aa.aa.aa.aa.aa.aa>] |mac-statistics [address
<aa.aa.aa.aa.aa.aa>] | all }]
```

Variable definitions

This table describes the variables used in the `show dot1x` command.

Variable	Value
all	Specifies the dot1x status for all interfaces.
interface	Specifies the dot1x status for the specified interface.
local-database	Specifies the dot1x authentication server database with user name and password.
mac-info	Specifies the dot1x MAC information for the interface with the specified MAC address.
mac-statistics	Specifies the dot1x MAC statistics for the interface with the specified MAC address.
statistics interface	Specifies the dot1x authenticator statistics for the switch or the specified interface.
supplicant-statistics interface	Specifies the dot1x supplicant statistics for the switch or the specified interface.

Related commands

`dot1x default`

shutdown dot1x

Use this command to shut down dot1x capability. Precede this command with no to start and enable dot1x capability.

Command mode

Global configuration

Syntax

```
shutdown dot1x
```

```
no shutdown dot1x
```

Related commands

dot1x system-auth-control

show dot1x

Remote Authentication Dial-in User Service commands

Remote Authentication Dial-in User Service (RADIUS) is a client and server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, and switches. RADIUS is the accepted standard for remote authentication. It is prevalent in both new and legacy systems and provides the following benefits:

- facilitates centralized user administration.
- consistently provides some level of protection against an active attacker.

RADIUS commands navigation

- debug radius (page 99)
- radius-server host (page 100)
- show radius server (page 101)
- show radius statistics (page 102)

debug radius

Use this command to enable the RADIUS debugging options. Precede this command with `no` to disable the RADIUS debugging options.

Command mode

Privileged EXEC

Syntax

```
debug radius {all | errors | events | packets | responses | timers}
```

```
no debug radius
```

Variable definitions

This table describes the variables used in the `debug radius` command.

Variable	Value
all	Enables all the RADIUS server messages.
errors	Enables error code debug messages.
events	Enables events related messages.
packets	Enables the packets related messages.
responses	Enables the server response related messages.
timers	Enables the timer related messages.

Defaults

Debugging is disabled

Related commands

`show radius server`

radius-server host

Use this command to configure the RADIUS client with the parameters which include host, timeout, key, and retransmit. Precede this command with no to delete the RADIUS server configuration.

Command mode

Global configuration

Syntax

```
radius-server host <ip-address> [timeout <1-120>] [retransmit <1-254>]
key <secret-key-string>


no radius-server host <ip address>
```

Variable definitions

This table describes the variables used in the `radius-server host` command.

Variable	Value
timeout	Specifies the time period in seconds for which a client will wait for a response from the server before re-transmitting the request.
retransmit	Specifies the maximum number of attempts the client undertakes to contact the server.
key	Specifies the per-server encryption key. Specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The string length is 46.

Defaults

timeout	10 seconds
retransmit	3 attempts
key	empty string

Related commands

`aaa authentication dot1x default`

`show radius server`

`show radius statistics`

show radius server

Use this command to display RADIUS server configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show radius server
```

Related commands

radius-server host

show radius statistics

Use this command to display RADIUS server statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show radius statistics
```

Related commands

`radius-server host`

TACACS commands

Terminal Access Controller Access Control System (TACACS) is a client and server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. Use this command to provide Network Access Security (NAS), which ensures secure access from remotely connected users. TACACS implements the TACACS client and provides the Authentication, Authorization, and Accounting (AAA) functionalities.

TACACS commands navigation

- debug tacacs (page 104)
- show tacacs (page 105)
- tacacs-server host (page 106)
- tacacs-server retransmit (page 107)
- tacacs use-server address (page 108)

debug tacacs

Use this command to set the debug trace level for TACACS client module. Precede the command with no to disable the debug trace level for TACACS client module.

Command mode

Privileged EXEC mode

Syntax

```
debug tacacs { all | info | errors | dumptx | dumprx }


no debug tacacs
```

Variable definitions

This table describes the variables used in the `debug tacacs` command.

Variable	Value
all	Displays all TACACS debug messages.
info	Displays TACACS server information messages.
errors	Displays error code debug messages.
dumptx	Displays transmitted packet dump messages.
dumprx	Displays received packet dump messages.

Defaults

Debugging is disabled

show tacacs

Use this command to view the statistical log information and server for TACACS+ client.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show tacacs
```

Related commands

`show tacacs`

`tacacs use-server address`

tacacs-server host

Use this command to configure host, timeout, and key in the TACACS server. Precede this command with `no` to delete the server entry from the TACACS server table.

Command mode

Global configuration mode.

Syntax

```
tacacs-server host <ip-address> [single-connection] [port <TCP
port(1-65535)>] [timeout <time out in seconds>] [key <secret key>]


no tacacs-server host <ip-address>
```

Variable definitions

This table describes the variables used in the `tacas-server host` command.

Variable	Value
single-connection	Establishes single TCP connection to communicate with TACACS server.
port	Enter TCP port number.
timeout	Enter the time period in seconds for which the client waits for a response from the server before closing the connection.
key	Enter the per-server encryption key. It describes the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The string length is 63.

Defaults

port	40
timeout	5 seconds

Related commands

`show tacacs`

tacacs-server retransmit

Use this command to get the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured. Precede the command with no to set the default retries.

Command mode

Global Configuration mode

Syntax

```
tacacs-server retransmit <retries>


no tacacs-server retransmit
```

Variable definitions

This table describes the variables used in the `tacacs-server retransmit` command.

Variable	Value
retries	Enter the number of times the client searches the active server. The value ranges from 1 to 100.

tacacs use-server address

Use this command to select a server from the list of servers maintained in the TACACS client and to force the TACACS client use the specified server. Precede this command with `no` to disable the TACACS active server.

Command mode

Global Configuration mode.

Syntax

```
tacacs use-server address<ip-address>


no tacacs use-server
```

Variable definitions

This table describes the variables used in the `tacacs use-server address` command.

Variable	Value
ip-address	Enter the IP address of the specified server.

Related Commands

`show tacacs`

Internet Group Management Protocol snooping commands

Internet Group Management Protocol (IGMP) is the protocol a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network. A router must use another multicast routing protocol to inform other routers of group membership. With the IGMP Snooping (IGS) feature, the switch can listen in on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops the IGMP data packets of the host computer, the other computer can learn the multicast sessions to which other computers on the local network are listening. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

IGMP commands navigation

- debug ip igmp snooping (page 110)
- ip igmp snooping (page 111)
- ip igmp snooping fast-leave (page 112)
- ip igmp snooping group-query-interval (page 113)
- ip igmp snooping mrouter (page 114)
- ip igmp snooping mrouter-time-out (page 115)
- ip igmp snooping port-purge-interval (page 116)
- ip igmp snooping proxy-reporting (page 117)
- ip igmp snooping querier (page 118)
- ip igmp snooping query-interval (page 119)
- ip igmp snooping report-forward (page 120)
- ip igmp snooping report-suppression-interval (page 121)
- ip igmp snooping retry-count (page 122)
- ip igmp snooping version (page 123)
- show ip igmp snooping (page 124)
- show ip igmp snooping forwarding-database (page 125)
- show ip igmp snooping globals (page 126)
- show ip igmp snooping groups (page 127)
- show ip igmp snooping mrouter (page 128)
- show ip igmp snooping statistics (page 129)
- shutdown snooping (page 130)
- snooping multicast-forwarding-mode (page 131)

debug ip igmp snooping

Use this command to specify the debug levels for IGMP snooping module. Precede this command with no to reset debug options for IGMP snooping module.

Command mode

Privileged EXEC

Syntax

```
debug ip igmp snooping {[init] [resources] [tmr] [src] [grp] [qry] [vlan]
[pkt] [fwd] [mgmt] [redundancy] | all }


no debug ip igmp snooping {[init] [resources] [tmr] [src] [grp] [qry]
[vlan] [pkt] [fwd] [mgmt] [redundancy] | all }
```

Variable definitions

This table describes the variables used in `debug ip igmp snooping` command.

Variable	Value
all	Displays all messages.
fwd	Displays forwarding database messages.
grp	Displays group information messages.
init	Displays initialize and shutdown messages
mgmt	Displays management related messages.
pkt	Displays packet dump messages.
qry	Displays query related messages.
redundancy	Displays redundancy related messages.
resources	Displays system resources management messages.
src	Displays source information messages.
tmr	Displays timer messages.
vlan	Displays VLAN information messages.

Defaults

Debugging is disabled

Related commands

`show debugging`

ip igmp snooping

Use this command to enable IGMP snooping in the switch or a specific VLAN. Precede this command with no to disable IGMP snooping in the switch or a specific VLAN. When IGMP snooping is globally enabled, it is enabled in all the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled in all the existing VLAN interfaces.

Command mode

Global configuration or config-VLAN

Syntax

```
ip igmp snooping


no ip igmp snooping
```

Defaults

IGMP snooping is globally disabled

Related commands

shutdown snooping

show ip igmp snooping

show ip igmp snooping globals

snooping multicast-forwarding-mode

ip igmp snooping fast-leave

Use this command to enable fast leave processing for a specific VLAN. Precede this command with no to disable fast leave processing for a specific VLAN.

Command mode

Config-VLAN

Syntax

```
ip igmp snooping fast-leave
```

```
no ip igmp snooping fast-leave
```

Defaults

Disabled

Related commands

`show ip igmp snooping`

ip igmp snooping group-query-interval

Use this command to set the time interval after which the switch sends a group specific query on a port. Precede this command with no to set the group specific query interval time to default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping group-query-interval <(2 - 5) seconds>


no ip igmp snooping group-query-interval
```

Defaults

2

Related commands

show ip igmp snooping globals

show ip igmp snooping groups

show ip igmp snooping statistics

ip igmp snooping mrouter

Use this command to configure statically the router ports for a VLAN. Precede this command with no to delete the statically configured router ports for a VLAN.

Command mode

Config-VLAN

Syntax

```
ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

Related commands

show ip igmp snooping mrouter

ip igmp snooping mrouter-time-out

Use this command to set the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received. Precede this command with no to set the IGMP snooping router port purge time-out to default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping mrouter-time-out <(60 - 600) seconds>
no ip igmp snooping mrouter-time-out
```

Defaults

125

Related commands

`show ip igmp snooping mrouter`

ip igmp snooping port-purge-interval

Use this command to set the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received. Precede this command with no to set the IGMP snooping port purge time to default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping port-purge-interval <(130 - 1225) seconds>


no ip igmp snooping port-purge-interval
```

Defaults

260

Related commands

`show ip igmp snooping globals`

ip igmp snooping proxy-reporting

Use this command to enable proxy reporting in the IGMP snooping switch. Precede this command with no to disable proxy reporting in the IGMP snooping switch.

Command mode

Global configuration

Syntax

```
ip igmp snooping proxy-reporting
```

```
no ip igmp snooping proxy-reporting
```

Defaults

Proxy-reporting is enabled

Related commands

`show ip igmp snooping globals`

ip igmp snooping querier

Use this command to configure the IGMP snooping switch as a querier for a specific VLAN. Precede this command with no to configure the IGMP snooping switch as nonquerier for a specific VLAN.

Command mode

Config-VLAN

Syntax

```
ip igmp snooping querier
```

```
no ip igmp snooping querier
```

Defaults

Non-querier

Related commands

`show ip igmp snooping`

ip igmp snooping query-interval

Use this command to set the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. Precede this command with no to set the IGMP querier interval to default value.

Command mode

Config-VLAN

Syntax

```
ip igmp snooping query-interval <(60 - 600) seconds>


no ip igmp snooping query-interval
```

Defaults

125

Related commands

`show ip igmp snooping`

ip igmp snooping report-forward

Use this command to specify if IGMP reports must be forwarded on all ports or router ports of a VLAN. Precede this command with no to set IGMP report-forwarding status to default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping report-forward {all-ports | router-ports}


no ip igmp snooping report-forward
```

Variable definitions

This table describes the variables used in `ip igmp snooping report-forward` command.

Variable	Value
all-ports	Specifies IGMP reports forwarded on all the ports of a VLAN.
router-ports	Specifies IGMP reports forwarded on router ports of a VLAN.

Defaults

router-ports

Related commands

`show ip igmp snooping globals`

ip igmp snooping report-suppression-interval

Use this command to set the IGMP snooping report-suppression time interval for which the IGMPv2 report messages for the same group will not get forwarded onto the router ports. Precede this command with no to set the IGMP snooping report-suppression interval time to the default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping report-suppression-interval <(1 - 25) seconds>


no ip igmp snooping report-suppression-interval
```

Defaults

5

Related commands

`show ip igmp snooping globals`

ip igmp snooping retry-count

Use this command to set the maximum number of group specific queries sent on a port on reception of a IGMPv2 leave message. Precede this command with no to set the number of group specific queries sent on a port on reception of leave message to default value.

Command mode

Global configuration

Syntax

```
ip igmp snooping retry-count <1 - 5>


no ip igmp snooping retry-count
```

Defaults

2

Related commands

show ip igmp snooping globals

ip igmp snooping version

Use this command to set the operating version of the IGMP snooping switch for a specific VLAN.

Command mode

Config-VLAN

Syntax

```
ip igmp snooping version {v1 | v2 | v3}
```

Variable definitions

This table describes the variables used in the `ip igmp snooping version` command.

Variable	Value
v1	Specifies IGMP snooping Version 1.
v2	Specifies IGMP snooping Version 2.
v3	Specifies IGMP snooping Version 3.

Defaults

v3

Related commands

`show ip igmp snooping`

show ip igmp snooping

Use this command to display IGMP snooping information for all VLANs or a specific VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping [vlan <vlan id>]
```

Variable definitions

This table describes the variables used in `show ip igmp snooping` command.

Variable	Value
vlan	Enter the VLAN ID.

Related commands

`ip igmp snooping`

`ip igmp snooping fast-leave`

`ip igmp snooping querier`

`ip igmp snooping query-interval`

`ip igmp snooping version`

show ip igmp snooping forwarding-database

Use this command to display the multicast forwarding entries for all VLANs or a specific VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping forwarding-database [vlan <vlan id>]
```

Variable definitions

This table describes the variables used in the `show ip igmp snooping forwarding-database` command.

Variable	Value
vlan	Enter the Vlan index value.

Related commands

`ip igmp snooping`

show ip igmp snooping globals

Use this command to display the IGMP snooping information for all VLANs or a specific VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping globals
```

Related commands

ip igmp snooping

ip igmp snooping port-purge-interval

ip igmp snooping proxy-reporting

ip igmp snooping report-forward

ip igmp snooping report-suppression-interval

ip igmp snooping retry-count

ip igmp snooping version

snooping multicast-forwarding-mode

show ip igmp snooping groups

Use this command to display IGMP group information for all VLANs or a specific VLAN or a specific VLAN and group address.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping groups [Vlan <vlan id> [Group <Address>]]
```

Variable definitions

This table describes the variables used in the `show ip igmp snooping groups` command.

Variable	Value
vlan	Specifies the vlan index value.
Group	Enter the group address of the vlan ID.

Related commands

`ip igmp snooping`

show ip igmp snooping mrouter

Use this command to display the router ports for a VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping mrouter [Vlan <vlan index>]
```

Variable definitions

This table describes the variables used in the `show ip igmp snooping mrouter` command.

Variable	Values
vlan	Specifies the vlan ID value.

Related commands

`ip igmp snooping mrouter`

show ip igmp snooping statistics

Use this command to display IGMP snooping statistics for all VLANs or a specific VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp snooping statistics [Vlan <vlan id>]
```

Variable definitions

This table describes the variables used in the `show ip igmp snooping statistics` command.

Variable	Value
vlan	Enter the Virtual Local Area Network (VLAN) identifier.

Related commands

`show ip igmp snooping`

`show ip igmp snooping globals`

`shutdown snooping`

`snooping multicast-forwarding-mode`

shutdown snooping

Use this command to shut down snooping in the switch. Precede this command with no to start and enable snooping in the switch. When shutdown, all resources acquired by the Snooping module are released to the system. For the IGS feature to be functional on the switch, the system-control status must be set as start and the state must be enabled.

Command mode

Global Configuration

Syntax

```
shutdown snooping
```

```
no shutdown snooping
```

Defaults

```
no shutdown snooping
```

Related commands

ip igmp snooping

snooping multicast-forwarding-mode

Use this command to specify the snooping multicast forwarding mode (IP based or MAC based).

Command mode

Global configuration

Syntax

```
snooping multicast-forwarding-mode {ip | mac}
```

Variable definitions

This table describes the variables used in the `snooping multicast-forwarding-mode` command.

Variable	Value
ip	Specifies the IP address based mode.
mac	Specifies the MAC address based mode.

Defaults

ip

Related commands

`show ip igmp snooping globals`

Syslog commands

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport that allows a computer to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. You can transmit syslog messages on a device without having to configure a receiver, or even having a receiver physically present.

Syslog commands navigation

- clear logs (page 133)
- cmdbuffs (page 134)
- logging (page 135)
- mailserver (page 137)
- receiver mail-id (page 138)
- sender mail-id (page 139)
- show email alerts (page 140)
- show logging (page 141)

clear logs

Use this command to clear the system syslog buffers.

Command mode

Global configuration

Syntax

```
clear logs
```

Related commands

cmdbuffs

logging

show logging

cmdbuffs

Use this command to configure the number of syslog buffers for a particular user.

Command mode

Global configuration

Syntax

```
cmdbuffs <user name> <no.of buffers (1-200)>
```

Variable definitions

This table describes the variables used in the `cmdbuffs` command.

Variable	Value
user name	Enter the user name.
no. of buffers	Enter the number of log buffers to be allocated in the system.

Defaults

50

Related commands

`logging`

`show logging`

logging

Use this command to enable Syslog server and configures the Syslog Server IP address, the log-level and other Syslog related parameters. Precede this command with no to disable Syslog server and re-sets the configured Syslog server IP address, the log-level, and other Syslog related parameters. The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.

The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

Command mode

Global configuration

Syntax

```
logging {<ip-address> | buffered <size (1-200)>  | console  | facility
{local0  | local1 | local2 | local3 | local4 | local5 | local6 | local7|}
| trap  [{<level (0-7)> | alerts | critical | debugging | emergencies |
errors |  informational | notification | warnings }] | on | flash}


no logging {<ip-address>  | buffered   | console  | facility |  trap | on
| flash}
```

Variable definitions

This table describes the variables used in the `logging` command.

Variable	Value
ip-address	Specifies the host IP address used as a Syslog server.
buffered	Specifies the limits syslog messages displayed from an internal buffer.
console	Limits messages logged to the console.
facility	Specifies the facility that is indicated in the message. Facilities can be local0, local1, local2, local3, local4, local5, local 6, local7, user.
trap	Specifies the trap messages.
alerts	Specifies the immediate action needed.
critical	Specifies the critical conditions.
debugging	Specifies the debugging messages.
emergencies	Specifies that system is unusable.
errors	Specifies the error conditions.
informational	Specifies the information messages.

Variable	Value
notification	Specifies the normal but significant messages.
warnings	Specifies the warning conditions.
on	Specifies that syslog is enabled.
flash	Specifies the Flash.

Defaults

logging	on
console	enabled
timestamp	enabled
trap	critical
buffered	50
facility	mail

Related commands

`show logging`

mailserver

Use this command to set the mail server IP address to be used for sending email alert messages. Precede this command with no to reset the mail server IP address used for sending email alert messages.

Command mode

Global configuration

Syntax

```
mailserver <ip-address>


no mailserver
```

Related commands

logging

show email alerts

receiver mail-id

Use this command to set the receiver mail id. Precede this command with no to delete the configured receiver mail id. Primarily, the mailserver must be configured for this command. The sender and receiver email-ids are mandatory to send email alert messages.

Command mode

Global configuration

Syntax

```
receiver mail-id <mail-id (100)>

no receiver mail-id
```

Defaults

admin@domainname.com

Related commands

logging

mailserver

sender mail-id

show email alerts

show logging

sender mail-id

Use this command to set the sender mail id. Precede this command with no to delete the configured sender mail id. Primarily, the mailserver must be configured for this command. The sender and receiver email-ids are mandatory to send email alert messages.

Command mode

Global configuration

Syntax

```
sender mail-id <mail-id (100)>


no sender mail-id
```

Defaults

syslog@domainname.com

Related commands

logging

mailserver

receiver mail-id

show email alerts

show logging

show email alerts

Use this command to display email alerts related configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show email alerts
```

Related commands

`mailserver`

`receiver mail-id`

`sender mail-id`

show logging

Use this command to display logging status and configuration information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show logging
```

Related commands

logging

Secure Shell commands

Secure Shell (SSH) is a protocol for secure remote logon and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol (TLP) provides server authentication, confidentiality, and integrity.
- The User Authentication Protocol (UAP) authenticates the client-side user to the server. It runs over the TLP.
- The Connection Protocol (CP) multiplexes the encrypted tunnel into several logical channels. It runs over the UAP.

The client sends a service request after a secure transport layer connection is established. A second service request is sent after user authentication is complete. This allows you to define new protocols that coexist with these protocols.

SSH commands navigation

- debug ssh (page 143)
- ip ssh (page 144)
- show ip ssh (page 145)

debug ssh

Use this command to set the given trace levels for SSH. Precede this command with no to reset the given SSH trace level.

Command mode

Privileged EXEC

Syntax

```
debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])


no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

Variable definitions

This table describes the variables used in the `debug ssh` command.

Variable	Value
all	Specifies the initialization and shutdown messages.
shut	Specifies the shutdown messages.
mgmt	Specifies the management messages.
data	Specifies the data path messages.
ctrl	Specifies the control plane messages.
dump	Specifies the packet dump messages.
resource	Specifies the messages related to all resources except buffers.
buffer	Specifies the buffer messages.

Defaults

Debugging is disabled

Related commands

`show ip ssh`

ip ssh

Use this command to enable SSH server on the device and also configures the various parameters associated with SSH server. Precede this command with no to disable SSH server on the device and also re-sets the various parameters associated with SSH server.

Command mode

Global configuration

Syntax

```
ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth
([hmac-md5] [hmac-sha1]) }
```

```
no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth
([hmac-md5] [hmac-sha1]) }
```

Variable definitions

This table describes the variables used in the `ip ssh` command.

Variable	Value
version compatibility	Specifies the support for the SSH protocol version.
cipher	Specifies the cipher-algorithm list.
auth	Specifies the public key authentication for incoming SSH sessions.

Defaults

version compatibility	false
cipher	3des-cbc
auth	hmac-sha1

Related commands

`show ip ssh`

show ip ssh

Use this command to display SSH server information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ssh
```

Related commands

ip ssh

Secure Sockets Layer commands

Secure Sockets Layer (SSL) is a protocol developed for transmitting private documents through the Internet. SSL uses a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https instead of http.

The SSL protocol provides privacy between two communicating applications (a client and a server) and authenticates the server and the client (optional). SSL requires a reliable transport protocol (for example, TCP) for data transmission and reception.

The advantage of the SSL protocol is that it is application protocol independent. A higher level application protocol, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), or Telnet, can layer on top of the SSL protocol transparently. The SSL protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, which ensures privacy.

SSL commands navigation

- debug ssl (page 147)
- ip http secure (page 148)
- show ip http secure server status (page 149)
- show ssl server-cert (page 150)
- ssl gen cert-req algo rsa sn (page 151)
- ssl server-cert (page 152)

debug ssl

Use this command to set the given debug levels for SSL. Precede this command with no to reset the given SSL debug level.

Command mode

Privileged EXEC

Syntax

```
debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])


no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

Variable definitions

This table describes the variables used in the `debug ssl` command.

Variable	Value
all	Specifies the initialization and shutdown messages.
shut	Specifies the shutdown messages.
mgmt	Specifies the management messages.
data	Specifies the data path messages.
ctrl	Specifies the control plane messages.
dump	Specifies the packet dump messages.
resource	Specifies the messages related to all resources except buffers.
buffer	Specifies the buffer messages.

Defaults

Debugging is disabled

Related commands

`show ip http secure server status`

ip http secure

Use this command to enable SSL server on the device. This command helps to configure ciphersuites and crypto keys. Precede this command with no to disable SSL server on the device and also disables ciphersuites and crypto key configuration.

Command mode

Global configuration

Syntax

```
ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha]
[rsa-des-sha] [rsa-3des-sha]
[dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] | crypto key rsa
[usage-keys (512|1024)] }
```

```
no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha]
[rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha]
[rsa-exp1024-des-sha] }
```

Variable definitions

This table describes the variables used in the `ip http secure` command.

Variable	Value
server	Specifies the SSL server.
ciphersuite	Configures the ciphersuite list.
crypto key rsa	Enter the usage key.

Defaults

ciphersuite	rsa-null-md5

Related commands

`show ip http secure server status`

`show ssl server-cert`

show ip http secure server status

Use this command to display SSL status and configuration information. Initially, http secure server, ciphersuite, crypto key must be configured.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip http secure server status
```

Related commands

`ip http secure`

`ssl gen cert-req algo rsa sn`

`ssl server-cert`

`show ssl server-cert`

show ssl server-cert

Use this command to display SSL server certificate.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ssl server-cert
```

Related commands

`ip http secure`

`show ip http secure server status`

`ssl gen cert-req algo rsa sn`

`ssl server-cert`

ssl gen cert-req algo rsa sn

Use this command to create a certificate request using RSA key pair and subject name.

Command mode

Privileged EXEC

Syntax

```
ssl gen cert-req algo rsa sn <SubjectName>
```

Variable definitions

This table describes the variables used in the `ssl gen cert-req algo rsa sn` command

Variable	Value
SubjectName	Identification of the switch (or) the switch's IP address.

Related commands

`show ip http secure server status`

`show ssl server-cert`

ssl server-cert

Use this command to configure the server cert, input in PEM format. It generates a certificate request, which can be submitted to a CA (Certificate Authority) to obtain the SSL certificate for the device.

Command mode

Privileged EXEC

Syntax

```
ssl server-cert
```

Related commands

`show ip http secure server status`

`show ssl server-cert`

System feature commands

SMB BSG 8x12 offers a rich set of system features to a user, such as logon services, copying or writing facilities, and duplex negotiation support. Some features have special hardware requirements and others have special design considerations. The related command links provide overview descriptions of the features and include specific information to consider when using these features.

Common Forwarding Agent (CFA) is a proprietary module, which acts as a common forwarder of packets between the Network Protocol Modules (NPM), the Data Link Layer Protocol Layer Modules (DLLPLM), and the device drivers. CFA provides central management of the generic parameters of all the interfaces in the system.

System feature commands navigation

- archive download-sw (page 155)
- archive select (page 156)
- authorized-manager ip-source (page 157)
- base-mac (page 159)
- cli console (page 160)
- clock set (page 161)
- copy (page 162)
- copy-file (page 163)
- copy logs (page 164)
- copy startup-config (page 165)
- debug-logging (page 166)
- default ip address allocation protocol (page 167)
- default management port ip address (page 168)
- default mode (page 169)
- default restore-file (page 170)
- default tr69 (page 171)
- default vlan mgmt port ip address (page 172)
- disable login (page 173)
- dump network status (page 174)
- enable login (page 175)
- erase (page 176)
- flowcontrol (page 177)
- jumbo frame support (page 178)
- interface (page 179)
- ip address (page 181)
- ip address—DHCP, RARP (page 182)
- ip address negotiated (page 183)

- ip http port (page 184)
- login authentication (page 185)
- mac-address (page 186)
- mtu frame size (page 187)
- network-type wan (page 188)
- private link (page 189)
- prompt (page 190)
- set bootdelay (page 191)
- set ip http (page 192)
- show authorized-managers (page 193)
- show clock (page 194)
- show debugging (page 195)
- show debug-logging (page 196)
- show files (page 197)
- show flow-control (page 198)
- show http server status (page 199)
- show ip interface (page 200)
- show interface mtu (page 201)
- show interfaces (page 202)
- show interfaces—counters (page 204)
- show management vlan (page 205)
- show nvram (page 206)
- show running config (page 207)
- show sub-system information (page 208)
- show system information (page 209)
- show tasks (page 210)
- show uplink rate-limit status (page 211)
- shutdown—physical/VLAN/port-channel/tunnel/PPP Interface (page 212)
- snmp trap link-status (page 213)
- switch name (page 214)
- switchport (page 215)
- system set factory default (page 216)
- tunnel checksum (page 217)
- tunnel mode (page 218)
- tunnel path-mtu-discovery (page 219)
- tunnel udlr (page 220)
- uplink rate limit (page 221)
- uplink rate limit enable / disable (page 222)
- write (page 223)

archive download-sw

Use this command to perform an image download operation using TFTP from a remote location.

Command mode

Privileged EXEC

Syntax

```
archive download-sw  /overwrite {tftp://ip-address/filename |
flash:filename}
```

Variable definitions

This table describes the variables used in the `archive download-sw` command.

Variable	Value
overwrite	Overwrites the software image in flash with the downloaded one.
tftp://ip-address/filename	Specifies the source URL alias for a network (tftp) file system.
flash:filename	Specifies the source URL alias for a local flash file system.

archive select

Use this command to select the image when you restart next.

Command mode

Privileged EXEC

Syntax

```
archive select {pack1 | pack2}
```

Variable definitions

This table describes the variables used in the `archive select` command.

Variable	Value
pack1	Specifies the image in pack1.
pack2	Specifies the image in pack2.

Related commands

show system information

authorized-manager ip-source

Use this command to configure an IP authorized manager. Precede this command with no to remove manager from authorized managers list.

Command mode

Global configuration

Syntax

```
authorized-manager ip-source <ip-address> [{<subnet-mask> | /
<prefix-length(1-32)>}] [interface [<interface-type <0/a-b, 0/c, ...>]
[<interface-type <0/a-b, 0/c, ...>]][ppp <a,b,c-d>][radio
<wireless-ap-id>/<radioid (1-2)>] [vlan <a,b or a-b or a,b,c-d>] [cpu0]
[service [snmp] [telnet] [http] [https] [ssh]]


no authorized-manager ip-source < ip-address > [{<subnet-mask > | /
<prefix-length(1-32)>}]
```

Variable definitions

This table describes the variables used in the `authorized-manager ip-source` command.

Variable	Value
ip-address	Specifies either the network or host address.
subnet-mask	Specifies the IP address mask to be applied.
prefix-length	Specifies the prefix length.
interface	Specifies the valid interfaces which includes physical ports (including type, slot, and port number).
vlan	Specifies the VLANs in which the IP authorized manager can reside.
cpu0	Specifies the Out of Band management interface.
service	Indicates service type. Service can be as follows: telnet ssh http https snmp.

Defaults

All services are allowed for the configured manager

Related commands

show authorized-managers

base-mac

Use this command to configure the base MAC address for the switch in the NVRAM.

Command mode

Global configuration

Syntax

```
base-mac <mac address>
```

Defaults

00:01:02:03:04:05

Related commands

`show nvram`

cli console

Use this command to enable the console CLI through a serial port. Precede this command with no to disable console CLI.

Command mode

Privileged EXEC

Syntax

```
cli console

no cli console
```

Defaults

enable

clock set

Use this command to manage the system clock.

Command mode

Privileged EXEC

Syntax

```
clock set hh:mm:ss day month year
```

Related commands

show clock

copy

Use this command to copy the configuration from a remote site to flash.

Command mode

Privileged EXEC

Syntax

```
copy {flash:filename | {ftp username:password | tftp } <server_ip>
<file_name> startup-config}
```

Variable definitions

This table describes the variables used in `copy` command.

Variable	Value
flash:filename	Specifies flash or remote site.
ftp username:password	Specifies username and password to use ftp.
tftp	Specifies the TFTP server.
server_ip	Specifies the IP address or host name of the server to receive the file.
file name	Specifies name assigned to the file on the server.
startup-config	Specifies the startup-config.

copy-file

Use this command to copy a file from a source remote site or flash to a destination remote site or flash.

Command mode

Privileged EXEC

Syntax

```
copy { tftp://ip-address/filename | flash: filename}{ tftp://ip-address/
filename | flash: filename}
```

Variable definitions

This table describes the variables used in the `copy-file` command.

Variable	Value
tftp	Copies a log file to a TFTP server. ip-address - enter IP address or host name of the TFTP server to receive the file. filename - enter the name assigned to the file on the server.
flash: filename	Enter the flash or remote site.

copy logs

Use this command to write the system logs to a remote site.

Command mode

Privileged EXEC

Syntax

```
copy logs tftp://ip-address/filename
```

Variable definitions

This table describes the variables used in the `copy logs` command.

Variable	Value
tftp	Copies a log file to a TFTP server. ip-address—the IP address or host name of the server to receive the file. filename—the name assigned to the file on the server.

copy startup-config

Use this command to back up the initial configuration in flash or at a remote location.

Command mode

Privileged EXEC

Syntax

```
copy startup-config {flash: filename | { ftp username:password | tftp }
<server_ip><file_name>
```

Variable definitions

This table describes the variables used in `copy startup-config` command.

Variable	Value
flash:filename	Specifies the flash or remote site.
ftp username:password	Specifies username and password to use ftp.
server_ip	Specifies IP address or host name of the server to receive the file.
tftp	Copies a file to a TFTP server.

debug-logging

Use this command to configure where debug logs are to be displayed. Precede this command with no to display debug logs in the console.

Command mode

Global configuration

Syntax

```
debug-logging {console | file}


no debug-logging
```

Variable definitions

This table describes the variables used in `debug-logging` command.

Variable	Value
console	Debug logs are displayed in the console.
file	Debug logs are displayed in the file.

Related commands

`show debugging`

`show debug-logging`

default ip address allocation protocol

Use this command to configure the protocol by which the default interface acquires its IP address.

Command mode

Global configuration

Syntax

```
default ip address allocation protocol {bootp | rarp | dhcp}
```

Variable definitions

This table describes the variables used in `default ip address allocation protocol` command.

Variable	Value
bootp	Specifies the bootp server.
rarp	Specifies the RARP server.
dhcp	Specifies the DHCP server.

Defaults

DHCP

Related commands

`default mode`

`show nvram`

default management port ip address

Use this command to configure the IP address and subnet mask for the default management interface.

Command mode

Global configuration

Syntax

```
default mgmt port ip address <ip-address> [ subnet-mask <subnet mask> ]
```

Variable definitions

This table describes the variables used in `default management ip address` command.

Variable	Value
ip—address	Specifies the IP address of the management interface.
subnet—mask	Specifies the subnet mask of the management interface.

Defaults

ip—address	10.0.0.1
subnet—mask	255.0.0.0

Related commands

`show nvram`

default mode

Use this command to configure the mode by which the default interface acquires its IP address.

Command mode

Global Configuration Mode

Syntax

```
default mode {manual | dynamic}
```

Variable definitions

This table describes the variables used in the `default mode` command.

Variable	Value
dynamic	Specifies the dynamic mode. If dynamic mode is selected, the default interface gets the IP address through the dynamic IP address configuration protocols such as RARP, BootP, and DHCP based on the configuration done in the default ip address allocation protocol command.
manual	Specifies the manual mode. If manual mode is selected, then the default interface takes the issDefaultAddr configured in the system.

Defaults

manual

Related commands

`show nvram`

`default ip address allocation protocol`

default restore-file

Use this command to configure the default restoration file.

Command mode

Global configuration

Syntax

```
default restore-file <filename>
```

Defaults

BSG.conf

Related commands

show nvram

default tr69

Use this command to enable or disable the TR69 module automatically turns on.

Command mode

Global configuration

Syntax

```
default tr69 { enabled | disabled }
```

Variable definitions

This table describes the variables used in the `default tr69` command.

Variable	Value
enable	Enables the TR69 module.
disable	Disables the TR69 module.

Defaults

`enabled`

default vlan mgmt port ip address

Use this command to configure the IP address and subnet mask for the default vlan interface.

Command mode

Global configuration

Syntax

```
default vlan mgmt ip address <ip-address> [ subnet-mask <subnet mask> ]
```

Variable definitions

This table describes the variables used in the `default vlan mgmt port ip address` command.

Variable	Value
ip address	Enter the IP address for the default vlan interface.
subnet-mask	Enter the subnet mask for the default vlan interface.

Defaults

ip address	10.0.0.1
subnet-mask	255.0.0.0

Related commands

show nvram

disable login

Use this command to disable the login prompt and password prompt.

Command mode

Global configuration

Syntax

```
disable login
```

dump network status

Use this command to display the network status.

Command mode

Privileged EXEC

Syntax

```
dump network status
```

enable login

Use this command to enable the login prompt and password prompt.

Command mode

Global configuration

Syntax

```
enable login
```

erase

Use this command to clear the contents of the startup configuration or sets parameters in NVRAM to default values.

Command mode

Privileged EXEC

Syntax

```
erase {startup-config | nvram | flash:filename}
```

Variable definitions

This table describes the variables used in `erase` command.

Variable	Value
flash:filename	Specifies the local system flash filename.
nvram	Specifies the non volatile RAM.
startup-config	Specifies the startup configuration file.

Related commands

`show nvram`

`show system information`

flowcontrol

Use this command to set the send or receive flow-control value for an interface.

If flowcontrol send is on for a device and if it detects any congestion at its end, then it notifies the link partner or the remote device of the congestion by sending a pause frame.

If flowcontrol receive is on for the remote device and it receives a pause frame, then it stops sending any data packets. This prevents any loss of data packets during the congestion period.

The receive off and send off keywords can be used to disable flow control.

Command mode

Interface configuration

Syntax

```
flowcontrol {send | receive} {on | off}
```

Variable definitions

This table describes the variables used in `flowcontrol` command.

Variable	Value
off	Turns-off the attached devices' (when used with receive) or the local ports' (when used with send) ability to send flow-control packets to an interface or to a remote device respectively.
on	If used with receive allows an interface to operate with the attached device to send flow control packets. If used with send the interface sends flowcontrol packets to a remote device if the device supports it.
receive	Interface to receive flow control packets from a remote device.
send	Interface to send flow control packets to a remote device.

Defaults

flowcontrol receive off

flowcontrol send off

Related commands

`show files`

`show interfaces`

jumbo frame support

Use this command to configure the jumbo frame support on the interface.

Command mode

Interface configuration

Syntax

```
jumbo frames support {enable | disable}
```

Defaults

disable

Related commands

show interfaces

interface

Use this command to select an interface to configure, which can be a physical interface or a port-channel interface or a VLAN interface or Out of Band (OOB) interface. Precede this command with no to delete a VLAN / port-channel / tunnel / OOB interface. When this command executes, the user enters the interface configuration mode for that interface.

Command mode

Global configuration

Syntax

```
interface {cpu0 | Vlan <vlan-id (1-4094)> | port-channel
<port-channel-id (1-65535)> | tunnel <tunnel-id (0-128)> |
<interface-type> <interface-id> | radio <wirelss-ap-id>/<radioid (1-2)>
| ppp <interface-number> | serial <t1e1-controller-number>/<timeslot> |
pvc <dsl-id>/<pvc-id> | dsl <dsl-modem-id> | multilink
<multilink-bundle-number>| fxo channel <fxo channel (1)> | fxs channel
<fxs channel (1-2)>}


no interface { Vlan <vlan-id(1-4094)>|
Port-Channel<port-channel-id(1-65535)> | tunnel <tunnel-id (0-128)> |
pvc <dsl-id>/<pvc-id> | ppp <ppp-id> | multilink
<multilink-bundle-number>}
```

Variable definitions

This table describes the variables used in the `interface` command.

Variable	Value
cpu0	Specifies the OOB management interface.
vlan	Specifies the VLAN identifier.
vlanMgmt	Specifies the VLAN management entity (only available when WGS is enabled in the switch.
port-channel	Specifies the port channel identifier.
tunnel	Specifies the tunnel identifier.
interface-type	Specifies the interface type. The interface type can be a gigabitethernet or a fastethernet interface.
interface-id	Specifies the physical interface ID including type, slot and port number.
radio	Specifies the radio interface.
ppp	Specifies the point-to-point protocol interface.
pvc	Specifies the private virtual connection interface.
dsl	Specifies the digital signal line.
multilink	Specifies the multilink PPP interface.

Variable	Value
fxo channel	Specifies the Foreign eXchange Office channel.
fxs channel	Specifies the Foreign eXchange Subscriber channel.

Defaults

Vlan	1
interface-type	eth0

Related commands

show interfaces

ip address

Use this command to set the IP address of an interface. Precede this command with `no` to reset the IP address for the given Interface.

Command mode

Interface configuration mode. This command is applicable in VLAN interface mode and OOB interface mode.

Syntax

```
ip address  <ip-address> <subnet-mask>


no ip address
```

Variable definitions

This table describes the variables used in `ip address` command.

Variable	Value
ip-address	Specifies the IP address.
subnet-mask	Subnet mask for the associated IP subnet.

Defaults

IP Address specified in nvram.txt

Related commands

`show ip interface`

`release`

`renew`

ip address—DHCP, RARP

Use this command to configure the current VLAN/OOB interface to dynamically acquire an IP address from the RARP/DHCP Server. Precede this command with no to reset the IP Address for the interface.

Command mode

Interface configuration mode. This command is applicable in VLAN interface mode and OOB interface mode.

Syntax

```
ip address  {dhcp | rarp}


no ip address
```

Variable definitions

This table describes the variables used in the ip address—DHCP, RARP command.

Variable	Value
dhcp	Specifies the DHCP server.
rarp	Specifies the RARP server.

Defaults

IP Address specified in nvram.txt

Related commands

release

renew

show ip dhcp client stats

ip address negotiated

Use this command to acquire IP address by negotiation and erases the previously configured IP for PPP virtual link and multilink PPP bundles.

Command mode

Multilink PPP interface configuration or PPP interface configuration

Syntax

```
ip address negotiated
```

ip http port

Use this command to set the HTTP port. Precede this command with no to the HTTP port.

Command mode

Global configuration

Syntax

```
ip http port <port-number(1-65535)>


no ip http port
```

Defaults

80

Related commands

set ip http

login authentication

Use this command to set the authentication method for user logins. Precede this command with no to set the authentication method for user logins to default values.

Command mode

Global configuration

Syntax

```
login authentication { local | {radius | tacacs } [fallback_to_local]}

no login authentication
```

Variable definitions

This table describes the variables used in the `login authentication` command.

Variable	Value
local	Specifies the local username database for authentication.
radius	Lists all RADIUS servers for authentication.
tacacs	Specifies the Terminal Access Controller Access Control System.

Defaults

`local`

Related commands

`show system information`

`username`

mac-address

Use this command to clone a MAC address on this interface.

Command mode

Ethernet interface configuration

Syntax

```
mac-address <aa:aa:aa:aa:aa:aa>

no mac-address
```

Related commands

switchport

network-type wan

mtu frame size

Use this command to configure the Maximum Transmission Unit (MTU) frame size for the interface.

Command mode

Interface configuration

Syntax

```
mtu <frame-size(90-9202)>
```

Defaults

1500

Related commands

show interfaces

show interface mtu

network-type wan

Use this command to configure the interface as a WAN interface.

Command mode

Interface configuration

Syntax

```
network-type wan


no network-type wan
```

private link

Use this command to configure that this WAN link connects to a private network, so that no default route can add for this link. Precede this command with no to specify that this WAN link connects to a public network, so that a default route can add for this link.

Command mode

Ethernet interface configuration or PPP interface configuration or multilink interface configuration

Syntax

```
private link
```

```
no private link
```

Related commands

network-type wan

prompt

Use this command to write the prompt text into NVRAM. Precede the command with no to write the default prompt text into NVRAM.

Command mode

Global configuration

Syntax

```
prompt { prompt text }


no prompt
```

Variable definitions

This table describes the variables used in the `prompt` command.

Variable	Value
prompt text	Enter the prompt text.

Defaults

BSG#

set bootdelay

Use this command to configure the bootdelay value. It is used only for debugging purpose.

Command mode

Privileged EXEC

Syntax

```
set bootdelay <number(2-10)>
```

Variable definitions

This table describes the variables used in the `set bootdelay` command.

Variable	Value
number	Specifies the delay value in seconds. The range is 2 to 10.

set ip http

Use this command to enable or disable HTTP.

Command mode

Global configuration

Syntax

```
set ip http {enable | disable}
```

Variable definitions

This table describes the variables used in the `set ip http` command.

Variable	Value
enable	Enables HTTP status in the system.
disable	Disables HTTP status in the system.

Defaults

`enable`

Related commands

`ip http port`

show authorized-managers

Use this command to display the configured authorized managers.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show authorized-managers [ip-source <ip address>]
```

Variable definitions

This table describes the variables used in the `show authorized-managers` command

Variable	Value
ip-source	Specifies either the network or the host address.

Related commands

`authorized-manager ip-source`

show clock

Use this command to display the system date and time.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show clock
```

Related commands

clock set

show debugging

Use this command to display the state of each debugging option.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show debugging
```

Related commands

`debug dot1x`

`debug ip dhcp client`

`debug ip dhcp relay`

`debug ip dhcp server`

`debug ip igmp snooping`

`radius-server host`

`debug spanning-tree`

`debug ssh`

`debug ssl`

`debug vlan`

show debug-logging

Use this command to display the debug logs stored in file.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show debug-logging
```

Defaults

manual

Related commands

debug-logging

show files

Use this command to display list of files present in the flash.

Command mode

Privileged EXEC

Syntax

```
show files
```

show flow-control

Use this command to display flow control information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show flow-control [interface <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show flow-control` command

Variable	Value
interface	Specifies gigabitethernet or fastethernet interface. Specifies physical interface ID including type, slot and port number.

Related commands

`flowcontrol`

`show interfaces`

show http server status

Use this command to view the http server status.

Command mode

Privileged EXEC or user EXEC

Syntax

```
show http server status
```

Related commands

ip http port

set ip http

show ip interface

Use this command to display the IP interface configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip interface [Vlan <vlan-id(1-4094)>]
```

Variable definitions

This table describes the variables used in `show ip interface` command.

Variable	Value
Vlan	Specifies the Vlan identifier. The value ranges from 1 to 4094.

Related commands

`interface`

`show interfaces`

show interface mtu

Use this command to show the Maximum Transmission Unit (MTU) of ports in the switch.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show interface mtu [{Vlan <vlan-id (1-4094)> | port-channel
<port-channel-id (1-65535)> | <interface-type> <interface-id> }]
```

Variable definitions

This table describes the variables used in the `show interface mtu` command

Variable	Value
vlan	Specifies the VLAN identifier.
port-channel	Specifies the port channel identifier.
interface-type	Specifies the interface type (fastethernet or gigabitethernet interface).
interface-id	Specifies the physical interface ID which includes type, slot and port number.

Related commands

`mtu frame size`

show interfaces

Use this command to display the interface status and configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show interfaces [{ [<interface-type> <interface-id>] [{ description |
storm-control | flowcontrol | capabilities | status }] | vlan
<vlan-id(1-4094)> | port-channel <port-channel-id (1-65535)> | tunnel
<tunnel-id (0-128)> | dsl <dsl-modem-id> | pvc <dsl-id/pvc-id> | radio
<wrls-ap/radio-id> | ppp <ppp-id(1-4094)> [config ] | multilink
<multilink-bundle-number> }]
```

Variable definitions

This table describes the variables used in `show interfaces` command.

Variable	Value
interface-type	Specifies the interface type (fastethernet or gigabitethernet interface).
interface-id	Specifies the physical interface ID including type, slot and port number.
description	Description about the interface.
storm-control	Specifies the broadcast, multicast, and unicast storm control suppression levels for an interface.
flowcontrol	Specifies the receive or send flow control value for an interface.
capabilities	Specifies the capabilities of the interface.
status	Specifies the status of the interface.
vlan	Specifies the VLAN identifier.
port-channel	Specifies the port channel identifier.
tunnel	Specifies the tunnel identifier.
dsl	Specifies the digital subscriber line.
pvc	Specifies the private virtual connection.
radio	Specifies the radio.
ppp	Specifies the point-to-point protocol.
multilink	Specifies the multilink PPP interface.

Related commands

`flowcontrol`

`interface`

`show files`

show interfaces—counters

Use this command to display the interface status and configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show interfaces [{ <interface-type> <interface-id> | vlan <short
(1-4094)> | tunnel <tunnel-id(0-128)> | multilink
<multilink-bundle-number> | ppp <ppp-id(1-4094)> }] counters
```

Variable definitions

This table describes the variables used in the `show interfaces—counters` command.

Variable	Value
interface-type	Specifies the interface type (fastethernet or gigabitethernet interface).
interface-id	Specifies the physical interface ID including type, slot and port number.
vlan	Specifies the VLAN identifier.
tunnel	Specifies the tunnel identifier.
multilink	Specifies the multilink bundle number.
ppp	Specifies the PPP identifier.
counters	Specifies various counters for the switch or for the specific interface.

Related commands

`show interfaces`

show management vlan

Use this command to the VLANs associated with the management interface.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show management vlan
```

show nvram

Use this command to display the current information stored in the NVRAM.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show nvram
```

Related commands

base-mac

default tr69

default mode

default restore-file

erase

login authentication

uplink rate limit

show running config

Use this command to display the current system information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show running config
```

Related commands

show vlan port config

show sub-system information

Use this command to view the sub-system information like the IP address, operation status, and version.

Command mode

Privileged or user EXEC

Syntax

```
show sub-system information [{wifi | voip | safenet}]
```

Variable definitions

This table describes the variables used in the `show sub-system information` command.

Variable	Value
sub-system information	Specifies the information of the sub-system. The information can either be wifi, voip, or safe net.
wifi	Indicates wireless LAN.
voip	Indicates voice over IP.
safenet	Indicates safenet.

show system information

Use this command to display system information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show system information
```

Related commands

erase

login authentication

uplink rate limit

show tasks

Use this command to display the task control block information.

Command mode

Privileged EXEC

Syntax

```
show tasks
```

show uplink rate-limit status

Use this command to display the uplink rate limit information.

Command mode

Privileged or User EXEC

Syntax

```
show uplink rate-limit status
```

Related commands

`uplink rate limit enable / disable`

shutdown—physical/VLAN/port-channel/tunnel/PPP Interface

Use this command to disable a physical interface, VLAN interface, port-channel interface, tunnel interface, or OOB interface. Precede this command with no to enable a physical interface, VLAN interface, port-channel interface, tunnel interface, or OOB interface.

Command mode

Interface configuration mode for a physical interface, port-channel, tunnel interface, or OOB interface.

VLAN interface mode for a VLAN interface.

Syntax

```
shutdown
no shutdown
```

Defaults

Physical interface eth0 is enabled

Interface VLAN 1 is enabled for a VLAN interface

Port-channel interface is disabled

Related commands

`interface`

`show interfaces`

snmp trap link-status

Use this command to enable trap generation on either the physical interface or the port-channel interface. Precede this command with no to disable trap generation on the respective interface.

Command mode

Interface configuration

Syntax

```
snmp trap link-status

no snmp trap link-status
```

Defaults

enabled

Related commands

show interfaces

switch name

Use this command to configure the switch name.

Command mode

Global configuration

Syntax

```
switch name <name>
```

Variable definitions

This table describes the variables used in the `switch name` command.

Variable	Value
name	Specifies the switch name.

Related commands

show system information

switchport

Use this command to configure the port as switch port. Precede the command with no to change a Layer 2 switch interface into a Layer 3 routed interface and erases all the Layer 2 configurations.

Command mode

Interface configuration

Syntax

```
switchport
```

```
no switchport
```

Defaults

switchport

Related commands

show ip interface

system set factory default

Use this command to remove BSG.conf, BSGnvram.txt.

Command mode

Privileged or user EXEC

Syntax

```
system set factory default
```

tunnel checksum

Use this command to enable end-to-end check summing of packets. Precede this command with no to disable end-to-end check summing of packets.

Command mode

Tunnel Mode

Syntax

```
tunnel checksum

no tunnel checksum
```

Defaults

disabled

Related commands

show interfaces

tunnel mode

Use this command to the tunnel interface associated parameters. Precede this command with no to delete the tunnel interface associated parameters.

Command mode

Tunnel Mode

Syntax

```
tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId
(1-2147483647)>] source <TnlSrcIP/IfName> [dest <TnlDestIP>]


no tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId
(1-2147483647)>] source <TnlSrcIP/IfName/IfIndex> [dest <TnlDestIP>]
```

Variable definitions

This table describes the variables used in the `tunnel mode` command.

Variable	Value
gre	Specifies the generic router encapsulation mode.
sixToFour	Specifies the 6to4 encapsulation mode.
isatap	Specifies the ISATAP encapsulation mode.
compat	Specifies the IPv6 auto compatible encapsulation mode.
ipv6ip	Specifies the IPv6 over IPv6 configured encapsulation mode.
config-id	Specifies an identifier to distinguish between multiple tunnels of the same encapsulation method, with same end-points.
source	Specifies the address of the local end point of the tunnel.
dest	Specifies the address of the remote end point of the tunnel.

Related commands

`show interfaces`

tunnel path-mtu-discovery

Use this command to enable path MTU discovery on tunnel. Precede this command with no to path MTU discovery on tunnel.

Command mode

Interface configuration

Syntax

```
tunnel path-mtu-discovery [age-timer{<integer(5-254)>|infinite}]

no tunnel path-mtu-discovery
```

Variable definitions

This table describes the variables used in the `tunnel path-mtu-discovery` command.

Variable	Value
age-timer	Specifies the timeout in minutes, after which the estimate of the PMTU is considered stale.
infinite	Specifies that detection in the PMTU increase is not done.

Defaults

disabled

Related commands

`show interfaces`

tunnel udlr

Use this command to associate tunnel with a unidirectional interface. Precede this command with no to associate tunnel with a bidirectional interface.

Command mode

Tunnel Mode

Syntax

```
tunnel udlr {receive-only | send-only}


no tunnel udlr
```

Variable definitions

This table describes the variables used in the `tunnel udlr` command.

Variable	Value
receive-only	Specifies that uni-directional tunnel is incoming.
send-only	Specifies that uni-directional tunnel is outgoing.

Related commands

`show interfaces`

uplink rate limit

Use this command to configure the output channel rate. This is applicable for WAN interfaces only.

Command mode

Ethernet interface configuration

Syntax

```
uplink rate limit <speed((100000-100000000) in bps)>
```

Related commands

`uplink rate limit enable / disable`

uplink rate limit enable / disable

Use this command to enable or disable the uplink rate limiting feature over WAN interfaces.

Command mode

Global configuration

Syntax

```
uplink rate limit {enable | disable}
```

Variable definitions

This table describes the variables used in the `uplink rate limit enable / disable` command.

Variable	Value
enable	Enables the uplink rate limiting feature.
disable	Disables the uplink rate limiting feature.

Related commands

`show uplink rate-limit status`

write

Use this command to write the running-config to a flash file, startup-configuration file or to a remote site.

Command mode

Privileged EXEC

Syntax

```
write { flash:filename | startup-config | ftp|??ip-address/filename }
```

Variable definitions

This table describes the variables used in the `write` command.

Variable	Value
flash:filename	Specifies the flash or remote site.
startup-config	Specifies the startup configuration. If this option is chosen, then the switch will start with the saved configuration on reboot.
ftp	Copies a file to a FTP server. • ip-address - the IP address or host name of the server to receive the file. • filename - the name assigned to the file on the server.

Defaults

`manual`

Related commands

`show nvram`

`show system information`

Power over Ethernet commands

Power over Ethernet (PoE) technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The advantage of this technology is that the installers need to run only a single Ethernet cable that carries both power and data to each device. IP telephones, wireless LAN access points, Web cams, Ethernet hubs, computers, and other appliances use this technology prominently. Access points (AP) and network devices can be easily located, thus decreasing installation costs.

PoE is standardized in IEEE 802.3af. This technology offers new options to system designers by providing economical and flexible deployment of network devices.

PoE commands navigation

- power inline (page 225)
- power inline priority (page 226)
- set poe (page 227)
- show power detail (page 228)
- show power inline (page 229)

power inline

Use this command to enable or disable POE on a port.

Command mode

Interface configuration

Syntax

```
power inline {auto | never}
```

Variable definitions

This table describes the variables used in the `power inline` command

Variable	Value
auto	Enables POE on a port.
never	Disables POE on a port.

Defaults

never

Related commands

`show power inline`

power inline priority

Use this command to set the POE port priority to critical, high, or low.

Command mode

Interface configuration

Syntax

```
power inline priority {critical | high | low }
```

Variable definitions

This table describes the variables used in the `power inline priority` command

Variable	Value
critical	Sets the POE port priority to critical.
high	Sets the POE port priority to high.
low	Sets the POE port priority to low.

Defaults

Power inline priority is set to low by default.

Related commands

`show power inline`

set poe

Use this command to enable or disable POE module in the switch.

Command mode

Global configuration

Syntax

```
set poe {enable | disable}
```

Variable definitions

This table describes the variables used in the `set poe` command

Variable	Value
enable	Enables POE module in the switch.
disable	Disables POE module in the switch.

Related commands

`show power detail`

show power detail

Use this command to display the POE power supply status.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show power detail
```

Related commands

`set poe`

show power inline

Use this command to display the power status for all or the specified POE interface.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show power inline [{<interface-type> <interface-id>}]
```

Variable definitions

This table describes the variables used in the `show power inline` command

Variable	Value
interface-type	Specifies the type of interface (fastethernet or gigabitethernet).
interface-id	Specifies the interface ID.

Related commands

`power inline`

`power inline priority`

System commands

Use the system commands to manage access permissions, mode access, and terminal configurations on BSG.

System commands include the following:

- alias (page 231)
- clear screen (page 232)
- close line vty (page 233)
- configure terminal (page 234)
- disable (page 235)
- enable (page 236)
- enable password (page 237)
- end (page 238)
- exec-timeout (page 239)
- exit (page 240)
- group (page 241)
- help (page 242)
- line (page 243)
- line configuration mode (page 244)
- listgroups (page 245)
- show users (page 245)
- lock (page 247)
- logout (page 248)
- moduser (page 249)
- pagination (page 250)
- password (page 251)
- run script (page 252)
- show aliases (page 253)
- show history (page 254)
- show line (page 255)
- show privilege (page 256)
- show users (page 257)
- username (page 258)

alias

Use this command to replace the given token by the given string. Precede this command with no to remove the alias created for the given string.

Command mode

Global configuration

Syntax

```
alias <replacement string> <token to be replaced>


no alias <alias>
```

Variable definitions

This table describes the variables used in the `alias` command

Variable	Value
replacement string	Specifies the replacement string.
token to be replaced	Specifies the abbreviated or short form of the replacement string.

Related commands

`show aliases`

clear screen

Use this command to clear the screen.

Command mode

All

Syntax

```
clear screen
```

close line vty

Use this command to close the specified line (Telnet/SSH connection).

Command mode

Privileged or user EXEC

Syntax

```
close line vty <vty number>
```

Variable definitions

This table describes the variables used in the `close line vty` command

Variable	Value
vty number	Specifies the line number.

Related commands

`show line`

configure terminal

Use this command to enter the configuration mode.

Command mode

Privileged EXEC

Syntax

```
configure terminal
```

Related commands

end

exit

disable

Use this command to turn off privileged commands.

Command mode

User EXEC

Syntax

```
disable [Privilege level to go to <0-15>]
```

Related commands

enable

enable

Use this command to turn on privileged commands.

Command mode

User EXEC

Syntax

```
enable [Enable Level <0-15>]
```

Variable definitions

This table describes the variables used in the `enable` command

Variable	Value
Enable Level	Specifies the level to enter the system.

Related commands

`disable`

enable password

Use this command to modify enable password parameters. Precede this command with no to disable enable password parameters.

Command mode

Global configuration

Syntax

```
enable password [level (1-15)] <LINE  'enable' password>

no enable password [level (1-15)]
```

Variable definitions

This table describes the variables used in the `enable password` command.

Variable	Value
level	Specifies the privilege level.

Related commands

`username`

end

Use this command to exit from configuration mode.

Command mode

All

Syntax

```
end
```

Related commands

exit

exec-timeout

Use this command to set EXEC timeout (in seconds) for line disconnection. Precede this command with no to clear EXEC timeout for line disconnection.

Command mode

Line configuration

Syntax

```
exec-timeout <integer (1-18000)>

no exec-timeout
```

Defaults

1800 seconds

Related commands

`line configuration mode`

exit

Use this command to exit the current configuration mode to the next highest configuration mode in the CLI.

Command mode

All

Syntax

```
exit
```

Related commands

end

group

Use this command to add a command group. Precede the command with no to delete a group from the CLI group database.

Command mode

Global configuration

Syntax

```
group <group-name> {system|vpn|wireless|12|13|security|access|voice}
{read-only|read-write|no-access}


no group <group-name>
```

Variable definitions

This table describes the variables used in the `group` command.

Variable	Value
group-name	Enter the group name.
system	Adds system functional group.
vpn	Adds VPN functional group.
wireless	Adds wireless functional group.
l2	Adds layer 2 functional group.
l3	Adds layer 2 functional group.
security	Adds security functional group.
access	Adds access functional group.
voice	Adds voice functional group.
read-only	Sets read-only access.
read-write	Sets read-write access.
no-access	Sets no access.

Related commands

listgroups

help

Use this command to display help for a particular command.

Command mode

All

Syntax

```
help [command ]
```

Variable definitions

This table describes the variables used in the `help` command.

Variable	Value
command	Specifies the privileged command.

line

Use this command to configure a console or a virtual terminal line.

Command mode

Global configuration

Syntax

```
line {console | vty}
```

Variable definitions

This table describes the variables used in the `line` command.

Variable	Value
console	Configures a console.
vty	Configures virtual terminal line.

Related commands

end

exit

show line

line configuration mode

Use this command to configure a console or virtual terminal line.

Command mode

Global configuration

Syntax

```
line {console | vty}
```

Variable definitions

This table describes the variables used in the `line` command

Variable	Value
console	Configures a console.
vty	Configures virtual terminal line.

Related commands

`end`

`exit`

`show line`

listgroups

Use this command to list all the valid groups, with their associated functional groups.

Command mode

Privileged EXEC

Syntax

```
listgroups
```

Related commands

show users

listuser

Use this command to list all valid users, along with their permissible mode.

Command mode

Privileged EXEC

Syntax

```
listuser
```

Related commands

`show users`

lock

Use this command to lock the CLI console. You may want to lock the console to prevent unauthorized users from gaining access to the CLI command shell.

Command mode

Privileged EXEC

Syntax

```
lock
```

logout

Use this command to exit from Privileged EXEC or User EXEC mode to SMB BSG login prompt in case of console session.

Command mode

User EXEC

Syntax

```
logout
```

moduser

Use this command to modify the parameters (groups, password) for a user.

Command mode

Global configuration

Syntax

```
moduser <user-name> [password <passwd>] [groups
<grp-name1,grp-name2,grp-name3,....>]
```

Variable definitions

This table describes the variables used in the `moduser` command.

Variable	Value
user-name	Modifies the user-name.
password	Modifies the password.
groups	Modifies the command groups.

Related commands

group

listgroups

pagination

Use this command to enable pagination. Precede the command with no to disable the pagination.

Command mode

Privileged EXEC

Syntax

```
pagination

no pagination
```

Related commands

show line

password

Use this command to enable or to disable the user login prompt.

Command mode

Privileged EXEC

Syntax

```
password {enable | disable}
```

Variable definitions

This table describes the variables used in the `password` command.

Variable	Value
enable	Enables the user login prompt.
disable	Disables the user login prompt.

Related commands

`username`

run script

Use this command to run CLI commands from the specified script file.

Command mode

Privileged EXEC

Syntax

```
run script <script file> [<output file>]
```

Variable definitions

This table describes the variables used in the `run script` command.

Variable	Value
script file	Specifies the script file to be executed.
output file	Specifies the output file.

show aliases

Use this command to display the aliases.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show aliases
```

Related commands

alias

show history

Use this command to display command list history.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show history
```

show line

Use this command to display TTY line information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show line [{console | vty <integer (1-10)>| summary}]
```

Variable definitions

This table describes the variables used in the `show line` command

Variable	Value
console	Displays the console.
vty	Displays the virtual terminal line
summary	Displays the summary.

Related commands

`line configuration mode`

show privilege

Use this command to show current user privilege level.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show privilege
```

show users

Use this command to display information about terminal lines.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show users
```

Related commands

show users

username

Use this command to create a user with specific group permission. Use double quotation marks around username if the username is a combination of alphanumeric and special characters. Precede this command with no to delete a user and disable the enable password for that user.

Command mode

Global configuration

Syntax

```
username <user-name> [password <password>] <groupname...>

no username <user-name>
```

Variable definitions

This table describes the variables used in the `username` command.

Variable	Value
user-name	Specifies the user name.
password	Specifies the password.
groupname	Specifies the group name of the user.

Related commands

`enable password`

RMON commands

Remote Monitoring (RMON) is a standard monitoring specification5 that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

RMON commands navigation

- rmon alarm (page 260)
- rmon collection history (page 262)
- rmon collection stats (page 263)
- rmon event (page 264)
- set rmon (page 265)
- show rmon (page 266)

rmon alarm

Use this command to set an alarm on a Management Information Base (MIB) object.The alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds configured before. Precede this command with `no` to delete the alarm configured on the MIB object.

Command mode

Global configuration

Syntax

```
rmon alarm <alarm-number> <mib-object-id (255)> <sample-interval-time
(1-65535)> {absolute | delta} rising-threshold <value (0-65535)>
<rising-event-number (1-65535)> falling-threshold <value (0-65535)>
<falling-event-number(1-65535)> [owner <ownername (127)>]


no rmon alarm <number (1-65535)>
```

Variable definitions

This table describes the variables used in the `rmon alarm` command.

Variable	Value
alarm-number	Enter the alarm number.
mib-object-id	Enter the MIB object identifier.
sample-interval-time	Enter the time in seconds during which the alarm monitors the MIB variable.
absolute	Use this parameter to test each MIB variable directly.
delta	Use this parameter to test change between samples of a variable.
rising-threshold	Enter the number at which the alarm is triggered.
falling-threshold value	Enter a number at which the alarm is reset.
rising-event-number	Enter the event number to trigger when the rising threshold exceeds its limit.
falling-event-number	Enter the event number to trigger when the falling threshold exceeds its limit.
owner	Specifies the owner of the alarm.

Related commands

`rmon collection stats`

`rmon event`

`show rmon`

rmon collection history

Use this command to enable history collection of interface statistics in the buckets for the specified time interval. Precede this command with no to disable the history collection on the interface.

Command mode

Interface configuration

Syntax

```
rmon collection history <index (1-65535)> [buckets <bucket-number
(1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]


no rmon collection history <index (1-65535)>
```

Variable definitions

This table describes the variables used in the `rmon collection history` command.

Variable	Value
index	Enter the value of history table index.
buckets	The maximum number of buckets desired for the RMON collection history group of statistics.
interval	Enter the number of seconds in each polling cycle.
owner	This is optional field. It allows the user to enter the name of the owner of the RMON group of statistics.

Defaults

bucket number	50
interval	1800 seconds
owner	monitor

Related commands

`show rmon`

rmon collection stats

Use this command to enable RMON statistics collection on the interface. Precede the command with no to disable RMON statistics collection on the interface.

Command mode

Interface configuration

Syntax

```
rmon collection stats <index (1-65535))> [owner <ownername (127)>]


no rmon collection stats <index (1-65535)>
```

Variable definitions

This table describes the variables used in the `rmon collection stats` command.

Variable	Value
index	Enter the statistics table index.
owner	This is an optional field. It allows the user to enter the name of the owner of the RMON group of statistics with a string length of 127.

Defaults

owner	monitor

Related commands

set rmon

rmon event

Use this command to add an event to the RMON event table. The added event is associated with an RMON event number. Precede the command with no to delete an event from the RMON event table.

Command mode

Global configuration

Syntax

```
rmon event <number (1-65535)> [description <event-description (127)>]
[log] [owner <ownername (40)>] [trap <community (127)>]


no rmon event <number (1-65535)>
```

Variable definitions

This table describes the variables used in the `rmon event` command.

Variable	Value
number	Enter the event number.
description	Provides the description of the event.
log	Use this parameter to generate a log entry.
owner	Specifies the owner of the event.
trap	Use this parameter to generate a trap. The SNMP community string needs to pass for the specified trap.

Related commands

`rmon alarm`

`show rmon`

`show snmp community`

set rmon

Use this command to enable or to disable the RMON feature.

Command mode

Global configuration

Syntax

```
set rmon { enable | disable }
```

Variable definitions

This table describes the variables used in the `set rmon` command.

Variable	Value
enable	Enables the RMON feature in the system.
disable	Disables the RMON feature in the system.

Defaults

RMON module is disabled

Related commands

show rmon

show rmon

Use this command to view the RMON statistics, alarms, events, and history configured on the interface.

Command mode

Privileged EXEC or User Exec

Syntax

```
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events]
[history [history-index (1-65535)]]
```

Variable definitions

This table describes the variables used in the `show rmon` command.

Variable	Value
statistics	Enter the configured stats index value.
alarms	Specifies the configured alarm.
events	Specifies the configured events.
history	Specifies the configured history index.

Related commands

`set rmon`

`rmon collection history`

`rmon collection stats`

`rmon event`

`rmon alarm`

Virtual local area network commands

Virtual Local Area Network (VLANs) is a group of devices on different physical LAN segments, which communicate with each other as if they were all on the same physical LAN segment, for example a network of computers that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

VLANs provide the following benefits for switched LAN:

- improved administration efficiency
- optimized broadcast/multicast activity
- enhanced network security

VLAN commands navigation

- debug vlan (page 269)
- group restricted (page 271)
- mac-address-table aging-time (page 272)
- mac-address-table static multicast (page 273)
- mac-address-table static unicast (page 275)
- map protocol (page 276)
- port protocol-vlan (page 277)
- ports (page 278)
- protocol-vlan (page 279)
- set garp timer (page 280)
- set gmrp (page 281)
- set gvrp (page 282)
- set port gmrp (page 283)
- set port gvrp (page 284)
- show garp timer (page 285)
- show mac-address-table (page 286)
- show mac-address-table aging-time (page 287)
- show mac-address-table count (page 288)
- show mac-address-table dynamic multicast (page 289)
- show mac-address-table dynamic unicast (page 290)
- show mac-address-table static multicast (page 291)
- show mac-address-table static unicast (page 292)
- show protocol-vlan (page 293)
- show vlan (page 294)
- show vlan device capabilities (page 295)
- show vlan device info (page 296)

- show vlan port config (page 297)
- show vlan protocols-group (page 298)
- shutdown garp (page 299)
- switchport acceptable-frame-type (page 300)
- switchport ingress-filter (page 301)
- switchport map protocols-group (page 302)
- switchport mode (page 303)
- switchport priority default (page 304)
- switchport pvid (page 305)
- vlan (page 306)
- vlan map-priority (page 307)
- vlan restricted (page 308)

debug vlan

Use this command to enable module-wise debug traces like forwarding, priority, GARP, GVRP, or GMRP. Precede this command with no to disable debugging.

Command mode

Privileged EXEC

Syntax

```
debug vlan [{fwd | priority | garp | gvrp | gmrp | redundancy} [initshut]
[mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]
```

```
no debug vlan [{fwd | priority | garp | gvrp | gmrp | redundancy}
[initshut][mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]
```

Variable definitions

This table describes the variables used in the `debug vlan` command.

Variable	Value
fwd	Specifies the forwarding module.
priority	Specifies the VLAN priority module.
garp	Specifies the GARP module.
gvrp	Specifies the GVRP module.
gmrp	Specifies the GMRP module.
initshut	Initialize and shutdown.
mgmt	Specifies the management.
data	Specifies the data path.
ctpl	Specifies the control plane.
dump	Specifies the packet dump.
os	Specifies the traces related to all resources except buffer.
failall	Specifies the all failures state.
buffer	Specifies the buffer.
all	Specifies all the traces.
redundancy	Specifies the redundancy related messages.

Defaults

disabled

Related commands

show vlan

group restricted

Use this command to enable or disable restricted group registration on the port.

Command mode

Interface configuration

Syntax

```
group restricted {enable | disable}
```

Variable definitions

This table describes the variables used in the `group restricted` command.

Variable	Value
enable	Enables restricted group registration.
disable	Disables restricted group registration.

Defaults

disable

Related commands

`show vlan port config`

mac-address-table aging-time

Use this command to set the maximum age of a dynamically learnt entry in the MAC address table. Precede this command with no to set the maximum age of an entry in the MAC address table to its default value.

Command mode

Global configuration

Syntax

```
mac-address-table aging-time <10-1000000 seconds>

no mac-address-table aging-time
```

Defaults

300

Related commands

`show mac-address-table aging-time`

mac-address-table static multicast

Use this command to configure a static multicast MAC address in the forwarding database. Precede this command with no to delete a configured static multicast MAC address from the forwarding database.

Command mode

Global configuration

Syntax

```
mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)> [recv-port <interface-type> <interface-id>] interface
([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c,
...>] [port-channel <a,b,c-d>]]) [forbidden-ports ([<interface-type> <0/
a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel
<a,b,c-d>]])[status {permanent | deleteOnReset | deleteOnTimeout }]


no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)> [recv-port <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `mac-address-table static multicast` command.

Variable	Value
aa:aa:aa:aa:aa:aa	Specifies the destination MAC address.
vlan	Specifies the VLAN identifier.
recv-port	Specifies the received port's interface type and ID.
interface	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
port-channel	Specifies the port channel ID.
forbidden-ports	Specifies the forbidden ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the forbidden ports interface type and ID (fastethernet type or gigabitethernet type).
status	Specifies the status of the static unicast entry.

Defaults

status	permanent

Related commands

show mac-address-table static multicast

mac-address-table static unicast

Use this command to configure a static unicast MAC address in the forwarding database. Precede this command with no to delete a configured static unicast MAC address from the forwarding database.

Command mode

Global configuration

Syntax

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)> [recv-port <interface-type> <interface-id>] interface
([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c,
...>] [port-channel <a,b,c-d>]) [status {permanent | deleteOnReset |
deleteOnTimeout }]


no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)> [recv-port <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `mac-address-table static unicast` command.

Variable	Value
aa:aa:aa:aa:aa:aa	Specifies the destination MAC address.
vlan	Specifies the VLAN identifier.
recv-port	Specifies the received port's interface type and ID.
interface	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
port-channel	Specifies the port channel ID.
status	Specifies the status of the static unicast entry.

Defaults

status	permanent

Related commands

show mac-address-table static unicast

map protocol

Use this command to configure the group ID for a specific encapsulation and protocol value combination. This command adds a protocol to a protocol group for protocol based VLAN learning. Precede this command with no to remove the protocol from the entire group.

Command mode

Global configuration

Syntax

```
map protocol  {ip | novell | netbios | appletalk | other <aa:aa or
aa:aa:aa:aa:aa>}  {enet-v2 | rfc1042 | llcOther | snap8021H | snapOther}
protocols-group <Group id>

no map protocol  {ip | novell | netbios | appletalk | other <aa:aa or
aa:aa:aa:aa:aa>}  {enet-v2 | rfc1042 | llcOther | snap8021H | snapOther}
```

Variable definitions

This table describes the variables used in the `map protocol` command.

Variable	Value
ip | novell | netbios | appletalk	Specifies the protocol types.
other	Specifies the MAC address of any other protocol type not included in the list.
enet-v2 | snap | llcOther | snap8021H | snapOther	Specifies the Encapsulation Frame Types.
protocols-group	Specifies the group ID.

Related commands

`show vlan`

`show vlan protocols-group`

port protocol-vlan

Use this command to enable port protocol based VLANs. Precede this command with no to disable port Protocol based VLANs.

Command mode

Interface configuration

Syntax

```
port protocol-vlan

no port protocol-vlan
```

Defaults

enabled

Related commands

show vlan port config

ports

Use this command to configure a static VLAN entry with the required member ports, untagged ports and forbidden ports.

Command mode

Config-VLAN

Syntax

```
ports ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/
c, ...>] [port-channel <a,b,c-d>]) [untagged <interface-type> <0/a-b, 0/
c, ...> [<interface-type> <0/a-b, 0/c, ...>] [port-channel <a,b,c-d>]]
[forbidden <interface-type> <0/a-b, 0/c, ...> [<interface-type> <0/a-b,
0/c, ...>] [port-channel <a,b,c-d>]] [name <vlan-name >]
```

Variable definitions

This table describes the variables used in the `ports` command.

Variable	Value
ports	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the member ports interface type and ID (fastethernet type or gigabitethernet type).
port-channel <a,b,c-d>	Specifies the port channel ID.
untagged	Specifies the untagged ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the untagged ports interface type and ID (fastethernet type or gigabitethernet type).
forbidden	Specifies the forbidden ports interface type and ID (fastethernet type or gigabitethernet type).
interface-type <0/a-b, 0/c, ...>	Specifies the forbidden ports interface type and ID (fastethernet type or gigabitethernet type).
name	Specifies the administratively assigned string used to identify the VLAN.

Related commands

`show vlan`

protocol-vlan

Use this command to enable protocol-VLAN based classification on all the ports. Precede this command with no to disable protocol-VLAN based classification on all ports.

Command mode

Global configuration

Syntax

```
protocol-vlan

no protocol-vlan
```

Defaults

enabled

Related commands

show protocol-vlan

show vlan device info

set garp timer

Use this command to configure the GARP join time, leave time, and leaveall time in milliseconds.

Command mode

Interface configuration

Syntax

```
set garp timer {join | leave | leaveall} <time in milliseconds>
```

Variable definitions

This table describes the variables used in the `set garp timer` command.

Variable	Value
join	Configures the join time.
leave	Configures the leave time.
leaveall	Configures the leaveall time.

Defaults

join	20
leave	60
leaveall	1000

Related commands

`show garp timer`

set gmrp

Use this command to enable or disable GMRP globally on the device.

Command mode

Global configuration

Syntax

```
set gmrp {enable | disable }
```

Variable definitions

This table describes the variables used in the `set gmrp` command.

Variable	Value
enable	Enables GMRP on the device.
disable	Disables GMRP on the device.

Defaults

`enable`

Related commands

`show vlan`

`show vlan device info`

set gvrp

Use this command to enable or disable GVRP on a global basis.

Command mode

Global configuration

Syntax

```
set gvrp {enable | disable }
```

Variable definitions

This table describes the variables used in the `set gvrp` command.

Variable	Value
enable	Enables GVRP in the switch.
disable	Disables GVRP in the switch.

Defaults

`enable`

Related commands

`show vlan`

`show vlan device info`

set port gmrp

Use this command to enable or disable GMRP on the port.

Command mode

Global configuration

Syntax

```
set port gmrp <interface-type> <interface-id> {enable | disable}
```

Variable definitions

This table describes the variables used in the `set port gmrp` command.

Variable	Value
interface-type	Specifies the interface type.
interface-id	Specifies the interface ID.
enable	Enables GMRP on the interface.
disable	Disables GMRP on the interface.

Defaults

`enable`

Related commands

`show vlan port config`

set port gvrp

Use this command to enable or disable GVRP on the interface.

Command mode

Global configuration

Syntax

```
set port gvrp <interface-type> <interface-id> {enable | disable}
```

Variable definitions

This table describes the variables used in the `set port gvrp` command.

Variable	Value
interface-type	Specifies the interface type.
interface-id	Specifies the interface ID.
enable	Enables GVRP on the interface.
disable	Disables GVRP on the interface.

Defaults

`enable`

Related commands

`show vlan port config`

show garp timer

Use this command to display the GARP timer information of the available interfaces.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show garp timer [port <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show garp timer` command.

Variable	Value
port	Specifies the interface type and port ID.

Related commands

`ports`

`set garp timer`

`show vlan device info`

show mac-address-table

Use this command to display the static and dynamic unicast and multicast MAC address table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table [vlan <vlan-id(1-4094)>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table` command.

Variable	Value
vlan	Specifies the VLAN ID.
address	Specifies the MAC address.
interface	Specifies the interface type and ID.

Related commands

`mac-address-table static multicast`

`mac-address-table static unicast`

`ports`

`vlan`

show mac-address-table aging-time

Use this command to display the MAC address-table ageing time.

Command mode

Privileged EXEC or User EXEC

Syntax

show mac-address-table aging-time

Related commands

show mac-address-table

mac-address-table aging-time

show mac-address-table count

Use this command to display the number of MAC addresses present on all the VLANs or on the specified VLAN.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table count [vlan <vlan-id(1-4094)>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table count` command.

Variable	Value
vlan	Specifies the VLAN ID.

Related commands

`mac-address-table static multicast`

`mac-address-table static unicast`

`ports`

`vlan`

show mac-address-table dynamic multicast

Use this command to display the dynamically learned multicast MAC address.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table dynamic multicast [vlan <vlan-id(1-4094)>]
[address <aa:aa:aa:aa:aa:aa>] [interface <interface-type>
<interface-id>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table dynamic multicast` command.

Variable	Value
vlan	Specifies the VLAN ID.
address	Specifies the MAC address.
interface	Specifies the interface type and ID.

Related commands

`mac-address-table static multicast`

`ports`

`show mac-address-table static multicast`

`vlan`

show mac-address-table dynamic unicast

Use this command to display the dynamically learned unicast entries from the MAC address table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table dynamic unicast [vlan <vlan-id(1-4094)>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table dynamic unicast` command.

Variable	Value
vlan	Specifies the VLAN ID. The value ranges from 1 to 4094.
address	Specifies the MAC address.
interface	Specifies the interface type and ID.

Related commands

`mac-address-table static unicast`

`ports`

`show mac-address-table static unicast`

`vlan`

show mac-address-table static multicast

Use this command to display the statically configured multicast entries.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table static multicast [vlan <vlan-id(1-4094)>]
[address <aa:aa:aa:aa:aa:aa>] [interface <interface-type>
<interface-id>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table static multicast` command.

Variable	Value
vlan	Specifies the VLAN ID. The value ranges from 1 to 4094.
address	Specifies the MAC address.
interface	Specifies the interface type and ID.

Related commands

`mac-address-table static multicast`

`ports`

`show mac-address-table dynamic multicast`

`vlan`

show mac-address-table static unicast

Use this command to display the statically configured unicast addresses from the MAC address table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-address-table static unicast [vlan <vlan-id(1-4094)>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show mac-address-table static unicast` command.

Variable	Value
vlan	Specifies the VLAN ID. The value ranges from 1 to 4094.
address	Specifies the MAC address.
interface	Specifies the Interface type and ID.

Related commands

`mac-address-table static unicast`

`ports`

`show mac-address-table dynamic unicast`

`vlan`

show protocol-vlan

Use this command to display the entries in protocol-VLAN database.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show protocol-vlan
```

Related commands

`switchport map protocols-group`

show vlan

Use this command to display the VLAN information in the database.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan [brief | id <vlan-id(1-4094)> | summary]
```

Variable definitions

This table describes the variables used in the `show vlan` command.

Variable	Value
brief	Specifies the brief information about all the VLANs.
id	Displays VLAN ID specific information.
summary	Displays VLAN summary.

Related commands

`ports`

`vlan`

show vlan device capabilities

Use this command to display the VLAN capabilities of the device.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan device capabilities
```

show vlan device info

Use this command to display the VLAN related global status variables.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan device info
```

Related commands

port protocol-vlan

ports

set gmrp

set gvrp

set port gmrp

set port gvrp

show protocol-vlan

vlan

show vlan port config

Use this command to display the VLAN related parameters specific for ports.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan port config [port <interface-type> <interface-id>]
```

Variable definitions

This table describes the variables used in the `show vlan port config` command.

Variable	Value
port	Specifies the interface type and port ID.

Related commands

`port protocol-vlan`

`set port gmrp`

`set port gvrp`

`switchport acceptable-frame-type`

`switchport ingress-filter`

`switchport pvid`

`vlan restricted`

show vlan protocols-group

Use this command to display the protocol group database.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan protocols-group
```

Related commands

`map protocol`

`show protocol-vlan`

`switchport map protocols-group`

shutdown garp

Use this command to command shut down the GARP module. Precede this command with no to start and enables the GARP module.

Command mode

Global configuration

Syntax

```
shutdown garp

no shutdown garp
```

Defaults

GARP module is started and enabled

switchport acceptable-frame-type

Use this command to configure the acceptable frame type for the port. Precede this command with no to set the default value of acceptable frame type (all frames will be accepted).

Command mode

Interface configuration

Syntax

```
switchport acceptable-frame-type {all | tagged}

no switchport acceptable-frame-type
```

Variable definitions

This table describes the variables used in the `switchport acceptable-frame-type` command.

Variable	Value
all	Configures all frames.
tagged	Configures tagged frames.

Defaults

all

Related commands

`show vlan port config`

switchport ingress-filter

Use this command to enable ingress filtering on the port. Precede this command with no to disable ingress filtering on the port.

Command mode

Interface configuration

Syntax

```
switchport ingress-filter

no switchport ingress-filter
```

Defaults

disabled

Related commands

show vlan port config

switchport map protocols-group

Use this command to map the protocol group configured to a particular VLAN identifier for the specified interface. Precede this command with no to unmap the VLAN identifier to group ID mapping.

Command mode

Interface configuration

Syntax

```
switchport map protocols-group <Group id> vlan <vlan-id(1-4094)>

no switchport map protocols-group <Group id>
```

Variable definitions

This table describes the variables used in the `switchport map protocols-group` command.

Variable	Value
Group id	Specifies the group ID to map.
vlan	Specifies the VLAN ID.

Related commands

`map protocol`

`show protocol-vlan`

`show vlan protocols-group`

switchport mode

Use this command to configure the VLAN port mode. Precede this command with no to configure the default VLAN port mode.

Command mode

Interface configuration

Syntax

```
switchport mode {access | trunk | hybrid }

no switchport mode
```

Variable definitions

This table describes the variables used in the `switchport mode` command.

Variable	Value
access	Specifies the access port mode.
trunk	Specifies the trunk port mode.
hybrid	Specifies the hybrid VLAN port mode.

Defaults

hybrid mode

Related commands

`show vlan port config`

switchport priority default

Use this command to set the default user priority for the port. Precede this command with no to set the default user priority for the port to the default value.

Command mode

Interface configuration

Syntax

```
switchport priority default <priority value(0-7)>

no switchport priority default
```

Defaults

0

Related commands

show vlan port config

switchport pvid

Use this command to configure the PVID (VLAN Identifier) that would be assigned to untagged or priority-tagged frames. Precede this command with no to set the PVID to the default value.

Command mode

Interface configuration

Syntax

```
switchport pvid <vlan-id(1-4094)>


no switchport pvid
```

Defaults

vlan-id	1

Related commands

show vlan port config

vlan

Use this command to configure a VLAN in the switch and is also used to enter into the config-VLAN mode. Precede this command with no to delete a VLAN from the switch.

Command mode

Global configuration

Syntax

```
vlan <vlan-id(1-4094)>


no vlan <vlan-id(1-4094)>
```

Defaults

vlan-id	1

Related commands

show vlan

vlan map-priority

Use this command to map a priority to a traffic class on the specified port. The frame received on the interface with the configured priority will be processed in the configured traffic class. Precede this command with no to map the default priority to traffic class value on the port.

Command mode

Interface configuration

Syntax

```
vlan map-priority <priority value(0-7)> traffic-class <Traffic class
value(0-7)>


no vlan map-priority <priority value (0-7)>
```

Variable definitions

This table describes the variables used in the `vlan map-priority` command.

Variable	Value
traffic-class	Specifies the traffic class value.

Defaults

vlan map priority	Default `traffic class`
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

vlan restricted

Use this command to enable or disable restricted VLAN registration on the port.

Command mode

Interface configuration

Syntax

```
vlan restricted {enable | disable}
```

Variable definitions

This table describes the variables used in the `vlan restricted` command.

Variable	Value
enable	Enables restricted VLAN registration.
disable	Disables restricted VLAN registration.

Defaults

disable

Related commands

`show vlan port config`

Dynamic host configuration protocol commands

Dynamic Host Configuration Protocol (DHCP) allows dynamic configuration of a host computer. When a DHCP client is turned on, it initially does not have an IP address assigned to it. It issues a broadcast message to any DCHP servers that are on the network. An exchange takes place during which the DHCP server assigns an IP address to the client and transmits certain key network configuration parameters to the client.

Many Internet service providers (ISPs) require that their customers use a DHCP client so the ISP can dynamically assign IP addresses and control other network settings. Another use is for laptop computers, which can be connected to more than one network, for example, a network in the office and a network at home. This is an ideal use for DHCP as the laptop does not need to be manually reconfigured for use in these two different networks. In this case, there must be a DHCP server both on the office network and the home network and the laptop requires a DHCP client.

DHCP client commands navigation

- debug ip dhcp client (page 311)
- ip address (page 312)
- release (page 313)
- renew (page 314)
- show ip dhcp client stats (page 315)

DHCP relay commands navigation

- debug ip dhcp relay (page 316)
- ip dhcp relay (page 317)
- ip dhcp relay information option (page 318)
- ip dhcp server (page 319)
- service dhcp-relay (page 320)
- show dhcp-server (page 321)
- show ip dhcp relay information (page 322)
- show ip dhcp relay interface (page 323)

DHCP server commands navigation

- debug ip dhcp server (page 324)
- default-router (page 325)
- dns-server (page 326)
- domain-name (page 327)
- excluded-address (page 328)
- host hardware-type (page 329)
- ip dhcp (page 330)
- ip dhcp bootfile (page 331)

- ip dhcp device (page 332)
- ip dhcp next-server (page 333)
- ip dhcp option (page 334)
- ip dhcp pool (page 335)
- lease (page 336)
- netbios-name-server (page 337)
- netbios-node-type (page 338)
- network (page 339)
- option (page 340)
- service dhcp-server (page 341)
- show ip dhcp server binding (page 342)
- show ip dhcp server devices (page 343)
- show ip dhcp server information (page 344)
- show ip dhcp server pools (page 345)
- show ip dhcp server statistics (page 346)
- show snmp-server traps (page 347)
- utilization threshold (page 348)

DHCP client commands

debug ip dhcp client

Use this command to set the debug level for tracing the DHCP client module. Precede this command with no to disable the debug level for the DHCP client.

Command mode

Privileged EXEC

Syntax

```
debug ip dhcp client {all | event | packets | errors | bind }

no debug ip dhcp client {all | event | packets | errors | bind }
```

Variable definitions

This table describes the variables used in the `debug ip dhcp client` command.

Variable	Value
all	Specifies the all trace messages.
event	Specifies the trace management messages.
packets	Specifies the packets related messages.
errors	Specifies the trace error code debug messages.
bind	Specifies the trace bind messages.

Defaults

Disabled

Related commands

`show ip dhcp client stats`

ip address

Use this command to configure the current virtual LAN (VLAN) or OOB interface to dynamically acquire an IP address from the DHCP server. Precede the command with no to reset the IP address for the interface.

Command mode

Interface configuration (VLAN interface or OOB interface)

Syntax

```
ip address dhcp
```

```
no ip address
```

Variable definitions

This table describes the variables used in the `ip address` command.

Variable	Value
dhcp	Indicates the DHCP server which provides the IP address.

Defaults

dhcp

Related commands

`show ip dhcp client stats`

`release`

`renew`

release

Use this command to immediately release the DHCP lease on the interface specified.

Command mode

Privileged EXEC

Syntax

```
release dhcp {vlan <vlan-id> (1-4094)>|<interface-name><interface-id>
```

Variable definitions

This table describes the variables used in the `release` command.

Variable	Value
vlan-id	Specifies the VLAN ID. The value ranges from 1 to 4094.
<interface-name><interface-id>	Specifies the interface type and interface identifier.

Defaults

Disabled

Related commands

`ip address`

`show ip dhcp client stats`

`show ip interface`

renew

Use this command to immediately renew the DHCP lease on the interface specified.

Command mode

Privileged EXEC or User EXEC

Syntax

```
renew dhcp vlan {<vlan-id (1-4094)> | <interface-type> <interface-id>}
```

Variable definitions

This table describes the variables used in the `renew` command.

Variable	Value
vlan-id	Specifies the VLAN ID. The value ranges from 1 to 4094.
<interface-type><interface-id>	Specifies the interface type and interface identifier.

Defaults

Disabled

Related commands

`ip address`

`show ip dhcp client stats`

show ip dhcp client stats

Use this command to display the DHCP client statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp client stats
```

Defaults

Disabled

Related commands

ip address

release

renew

DHCP relay commands

debug ip dhcp relay

Use this command to enable the debug level for tracing the DHCP relay module. Precede this command with no to disable the debug level for tracing the DHCP relay module.

Command mode

Privileged EXEC

Syntax

```
debug ip dhcp relay {all | errors}

no debug ip dhcp relay {all | errors}
```

Variable definitions

This table describes the variables used in the `debug ip dhcp relay` command.

Variable	Value
all	Specifies all trace messages.
errors	Specifies the trace error code debug messages.

Defaults

Disabled

Related commands

`show dhcp-server`

`show ip dhcp relay information`

ip dhcp relay

Use this command to enable or to disable the DHCP relay on the specified interface.

Command mode

Interface configuration

Syntax

```
ip dhcp relay {enable | disable}
```

Variable definitions

This table describes the variables used in the `ip dhcp relay` command.

Variable	Value
enable	Enables the DHCP relay.
disable	Disables the DHCP relay.

Defaults

enable

Related commands

`show ip dhcp relay interface`

ip dhcp relay information option

Use this command to enable the Relay Agent to perform any processing related to relay agent Information Options. When this option is enabled, the agent will insert and remove DHCP relay information in forwarded DHCP request messages to the DHCP server. Precede this command with no to disable the insertion of relay information.

Command mode

Global configuration

Syntax

```
ip dhcp relay information option

no ip dhcp relay information option
```

Defaults

Disabled

Related commands

`show dhcp-server`

`show ip dhcp relay information`

ip dhcp server

Use this command to set the IP address of the DHCP server. The relay agent will now start forwarding the packets from the client to a specific DHCP server. Precede this command with no to delete the DHCP server IP address.

Command mode

Global configuration

Syntax

```
ip dhcp server <ip address>

no ip dhcp server <ip address>
```

Defaults

Disabled

Related commands

show dhcp-server

show ip dhcp relay information

service dhcp-relay

Use this command to enable the DHCP Relay agent in the switch. Precede this command with no to disable the DHCP relay agent.

Command mode

Global configuration

Syntax

```
service dhcp-relay

no service dhcp-relay
```

Defaults

Disabled

Related commands

show dhcp-server

show ip dhcp relay information

show dhcp-server

Use this command to display the DHCP server information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dhcp-server
```

Related commands

`ip dhcp relay information option`

`ip dhcp server`

`service dhcp-relay`

show ip dhcp relay information

Use this command to display the DHCP relay information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp relay information
```

Related commands

`ip dhcp relay information option`

`ip dhcp server`

`service dhcp-relay`

show ip dhcp relay interface

Use this command to view the DHCP relay status on interfaces.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp relay interface [Vlan <vlan id>]
```

Variable definitions

This table describes the variables used in the `show ip dhcp relay interface` command.

Variable	Value
vlan id	Enter the VLAN ID.

Related commands

`ip dhcp relay`

DHCP server commands

debug ip dhcp server

Use this command to enable the debug level for tracing the DHCP server module. Precede this command with no to disable the debug level for tracing the DHCP server module.

Command mode

Privileged EXEC

Syntax

```
debug ip dhcp server {all | events | packets | errors | bind }

no debug ip dhcp server {all | events | packets | errors | bind }
```

Variable definitions

This table describes the variables used in the `debug ip dhcp server` command.

Variable	Value
all	Specifies all trace messages.
events	Specifies the trace management messages.
packets	Specifies the packet related messages.
errors	Specifies the trace error code debug messages.
bind	Specifies the trace bind messages.

Defaults

Debugging is disabled

Related commands

`show ip dhcp server binding`

`show ip dhcp server information`

`service dhcp-relay`

default-router

Use this command to set the default router in the DHCP server configuration parameters. Precede this command with no to delete the default router from the DHCP server configuration parameters.

Command mode

DHCP pool configuration

Syntax

```
default-router <ip address>

no default-router
```

Related commands

network

service dhcp-server

show ip dhcp server binding

show ip dhcp server information

show ip dhcp server pools

show ip dhcp server statistics

dns-server

Use this command to specify the IP address of a DNS server that is available to a DHCP client. Precede this command with no to delete the DNS server from the DHCP server configuration parameters.

Command mode

DHCP pool configuration

Syntax

```
dns-server <ip address>

no dns-server
```

Related commands

network

service dhcp-server

show ip dhcp server binding

show ip dhcp server information

show ip dhcp server pools

show ip dhcp server statistics

domain-name

Use this command to set the domain name in the DHCP server configuration parameters. Precede this command with no to delete the domain name from the DHCP server configuration parameters.

Command mode

DHCP pool configuration

Syntax

```
domain-name <domain (63)>

no domain-name
```

Variable definitions

This table describes the variables used in the `domain-name` command.

Variable	Value
domain	Specifies the client's domain name string.

Related commands

`network`

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

excluded-address

Use this command to create an excluded pool to prevent DHCP Server from assigning certain addresses. Precede this command with no to delete the excluded pool.

Command mode

DHCP pool configuration

Syntax

```
excluded-address <low-address> <high-address>

no excluded-address <low-address> [<high-address>]
```

Variable definitions

This table describes the variables used in the `excluded-address` command.

Variable	Value
low-address	Specifies the excluded IP address, or first IP address in an excluded address range.
high-address	Specifies the last IP address in the excluded address range.

Related commands

`network`

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

host hardware-type

Use this command to specify the hardware address of a DHCP client and host specific DHCP options. Precede this command with no to delete the host option.

Command mode

DHCP pool configuration

Syntax

```
host hardware-type <type (1-2147483647)> client-identifier <mac-address>
{ ip <address> [<identifier>] | option <code (1-2147483647)> { ascii
<string> | hex <Hex String> | ip <address> | integer <0-4294967295> }}


no host hardware-type <host-hardware-type (1-2147483647)>
client-identifier <client-mac-address> [{ ip |option <code
(1-2147483647)> }]
```

Variable definitions

This table describes the variables used in the `host hardware-type` command.

Variable	Value
type	Specifies the host hardware address type.
client identifier	Specifies the host MAC address.
ip	Specifies the IP address
identifier	Specifies the IP address identifier, which is a string of maximum length 63.
option	Specifies the tag octet of the DHCP option.
ascii	Specifies the ASCII string.
hex	Specifies the Hex string.
ip	Specifies the IP address.
integer	Specifies the integer.

Related commands

`service dhcp-server`

`ip dhcp pool`

ip dhcp

Use this command to set the DHCP server parameters such as enabling ICMP echo mechanism or offer-reuse timeout. Precede this command with no to set the DHCP server parameters like disabling ICMP echo mechanism or server offer-reuse to its default value or removing a bind entry from the server binding table.

Command mode

Global configuration

Syntax

```
ip dhcp {ping packets | server offer-reuse <timeout (1-120)> }

no ip dhcp {ping packets|server offer-reuse|binding <ip address>}
```

Variable definitions

This table describes the variables used in the `ip dhcp` command.

Variable	Value
ping packets	Enable icmp echo's prior to assigning a pool address. The no form of this command option prevents the server from pinging pool addresses.
server offer-reuse	Specifies the amount of time the DHCP server entity would wait for the DHCP request from the client before reusing the offer.
binding	Deletes the specified address from binding.

Defaults

ping packets	enabled
server offer-reuse	10

Related commands

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

ip dhcp bootfile

Use this command to set the boot file name in the DHCP server configuration parameters. Precede this command with no to delete the boot file name from the DHCP server configuration parameters.

Command mode

Global configuration

Syntax

```
ip dhcp bootfile <bootfile (63)>

no ip dhcp bootfile
```

Variable definitions

This table describes the variables used in the `ip dhcp bootfile` command.

Variable	Value
boot file	Name of the file that specifies the boot image.

Related commands

`service dhcp-server`

`show ip dhcp server information`

ip dhcp device

Use this command to configure the DHCP device name. Precede the command with no to delete the existing DHCP device name.

Command mode

Global configuration

Syntax

```
ip dhcp device <device-name (63)> [enable | disable]


no ip dhcp device <device-name (63)>
```

Variable definitions

This table describes the variables used in the `ip dhcp device` command.

Variable	Value
device-name	Enter the DHCP device name to configure. Maximum length of the device name string is 63.
enable	Enables the DHCP service to the specified device.
disable	Disables the DHCP service to the specified device.

Defaults

none

Related commands

show ip dhcp server devices

ip dhcp next-server

Use this command to set the next boot server in the DHCP server configuration parameters. Precede this command with no to delete the next boot server from the DHCP server configuration parameters.

Command mode

Global configuration

Syntax

```
ip dhcp next-server <ip address>

no ip dhcp next-server
```

Variable definitions

This table describes the variables used in the `ip dhcp next-server` command.

Variable	Value
ip address	Specifies the IP address of the TFTP server.

Related commands

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

ip dhcp option

Use this command to set the DHCP server options.

Command mode

Global configuration

Syntax

```
ip dhcp option <code (1-2147483647)> { ascii <string> | hex <Hex String>
| ip <address> | integer <integer (0-4294967295) }

no ip dhcp option <code (1-2147483647)>
```

Variable definitions

This table describes the variables used in the `ip dhcp option` command.

Variable	Value
code	Specifies the option code.
ascii	Specifies the ASCII string.
hex	Specifies the hexadecimal string.
ip	Specifies the IP address.
integer	Specifies the integer.

Related commands

`option`

`service dhcp-server`

`show ip dhcp server pools`

ip dhcp pool

Use this command to create a DHCP server address pool and to place the user in the DHCP pool configuration mode. Precede this command with no to delete the DHCP server address pool.

Command mode

Global configuration

Syntax

```
ip dhcp pool <index (1-2147483647)>

no ip dhcp pool <index (1-2147483647)>
```

Variable definitions

This table describes the variables used in the `ip dhcp pool` command.

Variable	Value
index	Specifies the pool number.

Defaults

Address pools are not created

Related commands

`default-router`

`dns-server`

`domain-name`

`excluded-address`

`host hardware-type`

`lease`

`netbios-name-server`

`netbios-node-type`

`network`

`option`

`show ip dhcp server information`

`show ip dhcp server pools`

lease

Use this command to configure the duration of the lease for an IP address that is assigned from the Nortel DHCP server to a DHCP client. Precede this command with no to restore the default value of 3600 seconds.

Command mode

DHCP pool configuration

Syntax

```
lease {<days (0-365)> [<hours (0-23)> [<minutes (0-59)>]] | infinite}

no lease
```

Variable definitions

This table describes the variables used in the `lease` command.

Variable	Value
days	Specifies the number of days in lease.
hours	Specifies the number of hours in lease.
minutes	Specifies the number of minutes in lease.
infinite	Specifies that the duration of the lease is unlimited.

Defaults

3600 seconds

Related commands

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

netbios-name-server

Use this command to set the NetBIOS (WINS) name servers in the DHCP server configuration parameters. Precede this command with no to delete the NetBIOS name server from the DHCP configuration parameters.

Command mode

DHCP pool configuration

Syntax

```
netbios-name-server <ip address>

no netbios-name-server
```

Related commands

network

service dhcp-server

show ip dhcp server binding

show ip dhcp server information

show ip dhcp server pools

show ip dhcp server statistics

netbios-node-type

Use this command to set the NetBios node type in the DHCP server configuration parameters. Precede this command with no to delete the NetBios node type from the DHCP server configuration parameters.

The NetBIOS node type for Microsoft DHCP clients can be one of the four settings: broadcast, peer-to-peer, mixed, or hybrid.

Command mode

DHCP pool configuration

Syntax

```
netbios-node-type {<0-FF> | b-node | h-node | m-node | p-node }

no netbios-node-type
```

Variable definitions

This table describes the variables used in the `netbios-node-type` command.

Variable	Value
0-FF	Specifies the node type value.
b-node	Specifies the broadcast node.
h-node	Specifies the hybrid node.
m-node	Specifies the mixed node.
p-node	Specifies the peer-to-peer node.

Related commands

`network`

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

network

Use this command to set the network IP address and mask in DHCP server configuration parameters. Precede this command with no to delete the network IP address and mask from DHCP server configuration.

Command mode

DHCP pool configuration

Syntax

```
network <network-IP> [{<mask> | / <prefix-length (1-31)> } ] [end ip]

no network
```

Variable definitions

This table describes the variables used in the `network` command.

Variable	Value
network-IP	Specifies the network IP address of the DHCP pool.
mask	Specifies the subnet mask of the DHCP pool.
prefix-length	Specifies the number of bits that comprise the address prefix. Prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
end ip	Specifies the end IP address of the pool.

Related commands

`service dhcp-server`

`show ip dhcp server binding`

`show ip dhcp server information`

`show ip dhcp server pools`

`show ip dhcp server statistics`

option

Use this command to the pool specific DHCP server option. Precede this command with no to delete the pool specific DHCP server option.

Command mode

DHCP pool configuration

Syntax

```
option <code (1-2147483647)> {ascii <string> | hex <Hex String> | ip
<address> | integer (0-4294967295)}


no option <code (1-2147483647)>
```

Variable definitions

This table describes the variables used in the `option` command.

Variable	Value
code	Specifies the value of the option code. The value ranges from 1 to 2147483647.
ascii	Specifies the ASCII string.
hex	Specifies the hexadecimal string.
ip	Specifies the IP address.
integer	Specifies the integer.

Related commands

`network`

`ip dhcp option`

`ip dhcp pool`

`service dhcp-server`

`show ip dhcp server pools`

service dhcp-server

Use this command to enable the DHCP server. Precede this command with no to disable the DHCP server.

Command mode

Global configuration

Syntax

```
service dhcp-server

no service dhcp-server
```

Defaults

Disabled

Related commands

`show ip dhcp server information`

show ip dhcp server binding

Use this command to display DHCP server binding information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp server binding
```

Related commands

`host hardware-type`

`ip dhcp option`

`service dhcp-server`

show ip dhcp server devices

Use this command to view the DHCP devices.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp server devices
```

Related commands

ip dhcp device

show ip dhcp server information

Use this command to display DHCP server information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp server information
```

Related commands

ip dhcp

ip dhcp bootfile

ip dhcp next-server

service dhcp-server

show ip dhcp server pools

Use this command to display DHCP server pools.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp server pools
```

Related commands

`ip dhcp pool`

`lease`

`network`

`service dhcp-server`

show ip dhcp server statistics

Use this command to display DHCP server statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip dhcp server statistics
```

Related commands

ip dhcp

ip dhcp pool

service dhcp-server

show ip dhcp server pools

show snmp-server traps

Use this command to view the set of traps that are currently enabled.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp-server traps
```

utilization threshold

Use this command to set the pool utilization threshold value in percentage. If the pool utilization reaches this threshold level, a syslog event and SNMP trap message will be generated. Precede the command with no to set pool utilization threshold to its default value.

Command mode

DHCP pool configuration

Syntax

```
utilization threshold { <integer (0-100)> }


no utilization threshold
```

Defaults

75

Related commands

show ip dhcp server pools

logging

Simple Network Management Protocol version 3 commands

Simple Network Management Protocol (SNMP) is the most widely used network management protocol on TCP/IP based networks. SNMPv3 is designed to overcome the security shortcomings of SNMPv1/v2. User-based Security Model (USM) and View-based Access Control Model (VACM) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP power distribution units (PDUs), while VACM specifies a mechanism for defining access policies for different users with different Management Information Base (MIB) trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new management engines, security models, and access control models. With SNMPv3, the SNMP communication is completely safe and secure.

SNMPv3 is a multilingual agent supporting all three versions of SNMP (SNMPv1, SNMPv2, and SNMPv3) while conforming to the latest specifications. It is available as a portable source code product, which can be easily integrated on any platform (any operating system and any processor). MIB integration is achieved through the use of the Middle Level Code Generator (MIDGEN), which is available along with Nortel SNMP. MIDGEN generates the interface stubs required for every object in the MIB for the SET, GET and GETNEXT operations.

These stubs can be implemented by the respective modules supporting the MIB. Nortel SNMP is provided as source code available for licensing to Original Equipment Manufacturers (OEMs) and Value Added Resellers (VARs) who want to incorporate the multilingual SNMP functionality into their products.

SNMPv3 commands navigation

- show snmp (page 351)
- show snmp agent information (page 352)
- show snmp community (page 353)
- show snmp engineID (page 354)
- show snmp group (page 355)
- show snmp group access (page 356)
- show snmp inform statistics (page 357)
- show snmp notif (page 358)
- show snmp-server traps (page 359)
- show snmp targetaddr (page 360)
- show snmp targetparam (page 361)
- show snmp user (page 362)
- show snmp viewtree (page 363)
- snmp agent status (page 364)
- snmp agent status (page 364)
- snmp allowed version (page 365)
- snmp community index (page 368)
- snmp engineid (page 370)
- snmp group (page 371)

- snmp notify (page 372)
- snmp-server enable traps snmp authentication (page 373)
- snmp targetaddr (page 374)
- snmp targetparams (page 376)
- snmp user (page 378)
- snmp view (page 379)
- snmp-server enable traps (page 380)
- system contact (page 381)
- system location (page 382)

show snmp

Use this command to display the status information of SNMP communications.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp
```

show snmp agent information

Use this command to display the SNMP agent information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp agent information
```

show snmp community

Use this command to display the configured SNMP community details.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp community
```

Related commands

`snmp community index`

show snmp engineID

Use this command to display the engine identifier.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp engineid
```

Related commands

snmp engineid

show snmp group

Use this command to display the configured SNMP groups.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp group
```

Related commands

`snmp group`
`snmp user`

show snmp group access

Use this command to the configured SNMP group access details.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp group access
```

Related commands

snmp agent status

snmp view

show snmp inform statistics

Use this command to display the inform message statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp inform statistics
```

show snmp notif

Use this command to display the configured SNMP notification types.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp notif
```

Related commands

snmp notify

snmp targetparams

show snmp-server traps

Use this command to display the set of traps that are currently enabled.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp-server traps
```

show snmp targetaddr

Use this command to display the configured SNMP target addresses.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp targetaddr
```

Related commands

snmp notify
snmp targetaddr
snmp targetparams

show snmp targetparam

Use this command to display the configured SNMP target address parameters.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp targetparam
```

Related commands

snmp targetparams

snmp user

show snmp user

Use this command to display the configured SNMP users.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp user
```

Related commands

`show snmp community`

`snmp user`

show snmp viewtree

Use this command to display the configured SNMP Tree views.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show snmp viewtree
```

Related commands

snmp view

snmp agent status

Use this command to enable or disable the SNMP agent status.

Command mode

Global configuration

Syntax

```
snmp agent status { enable | disable}
```

Variable definitions

This table describes the variables used in the `snmp agent status` command.

Variable	Value
enable	Enables the SNMP agent status.
disable	Disables the SNMP agent status.

Related commands

`show snmp agent information`

snmp allowed version

Use this command to configure the SNMP allowed versions.

Command mode

Global configuration

Syntax

```
snmp allowed version {v1v2v3 |v1v2 | v3 {none | authenticated |
encrypted}}
```

Variable definitions

This table describes the variables used in the `snmp allowed version` command.

Variable	Value
v1v2v3	Specifies the allowed SNMP v1, v2, and v3 versions.
v1v2	Specifies the allowed SNMP v1 and v2 versions.
v3	Specifies the allowed SNMP v3 versions.
none	Specifies that the SNMP version is without security.
authenticated	Specifies the SNMP version for authentication.
encrypted	Specifies the SNMP version for encryption.

Related commands

show snmp agent information

snmp access

Use this command to configure the SNMP group access details. Precede this command with no to remove the SNMP group access details.

Command mode

Global configuration

Syntax

```
snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read
<ReadView | none>] [write <WriteView | none>] [notify <NotifyView |
none>] [{volatile | nonvolatile}]

no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
```

Variable definitions

This table describes the variables used in the `snmp access` command.

Variable	Value
GroupName	Specifies the name of the SNMP group.
v1 | v2c | v3	Specifies the SNMP version.
auth	Specifies the authentication. The authentication enables Message Digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
noauth	Specifies the no authentication mode.
priv	Specifies both authentication and privacy.
read	Specifies a read view identifier.
write	Specifies a write view identifier.
notify	Specifies a notification view identifier.
volatile | nonvolatile	Specifies the storage type.

Defaults

GroupName	iso
Read/Write/Notify view	iso
StorageType	volatile
GroupName	initial
Read/Write/Notify view	restricted
StorageType	non-volatile
GroupName	initial
Read/Write/Notify view	iso
StorageType	non-volatile

Related commands

`show snmp group`

`show snmp group access`

`show snmp viewtree`

`snmp group`

`snmp view`

snmp community index

Use this command to configure the SNMP community details. Precede this command with no to remove the SNMP community details.

Command mode

Global configuration

Syntax

```
snmp community index <CommunityIndex> name <CommunityName> security
<SecurityName> [context <ContextName | none>] [{volatile | nonvolatile}]
[transporttag <TransportTagIdentifier | none>]


no snmp community index <CommunityIndex>
```

Variable definitions

This table describes the variables used in the `snmp community index` command.

Variable	Value
CommunityIndex	Specifies the community index identifier.
name	Specifies the community name.
security	Specifies the user name.
context	Specifies the context name through which the management information is accessed when using the community string specified by the corresponding instance of SNMP community name.
volatile | nonvolatile	Specifies the storage type.
transporttag	Specifies the transport tag identifier.

Defaults

CommunityIndex	NETMAN/PUBLIC
CommunityName	NETMAN/PUBLIC
SecurityName	None
ContextName	Null
TransportTag	Null
Storage type	Volatile

Related commands

`show snmp`

```
show snmp community
```

snmp engineid

Use this command to configure the engine identifier. Precede this command with no to remove the configured engine identifier.

Command mode

Global configuration

Syntax

```
snmp engineid <EngineIdentifier>

no snmp engineid
```

Variable definitions

This table describes the variables used in the `snmp engineid` command.

Variable	Value
EngineIdentifier	Specifies the engine ID to be configured.

Defaults

80.00.08.1c.04.46.53

Related commands

`show snmp engineID`

`show snmp user`

snmp group

Use this command to configure SNMP group details. Precede this command with no to remove the SNMP group details.

Command mode

Global configuration

Syntax

```
snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }
[{volatile | nonvolatile}]

no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }
```

Variable definitions

This table describes the variables used in the `snmp group` command.

Variable	Value
GroupName	Specifies the name of the SNMP group to be configured.
user	Specifies the user name.
security-model	Specifies the security model.
volatile | nonvolatile	Specifies the storage type.

Defaults

GroupName	iso/initial

Related commands

`show snmp group`

`show snmp user`

snmp notify

Use this command to configure the SNMP notification details. Precede this command with no to remove the SNMP notification details.

Command mode

Global configuration

Syntax

```
snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]


no snmp notify <NotifyName>
```

Variable definitions

This table describes the variables used in the `snmp notify` command.

Variable	Value
NotifyName	Specifies the notification name to be configured to get the detail.
tag	Specifies the tag name.
type	Specifies the notification type.
volatile | nonvolatile	Specifies the storage type of the notification details.

Defaults

NotifyName	iss/iss1
Notify tag	iss/iss1
Storage type	volatile

Related commands

`show snmp notif`

`show snmp targetaddr`

snmp-server enable traps snmp authentication

Use this command to enable generation of authentication traps for SNMPv1 and SNMPv2c. Precede this command with no to disable generation of authentication traps for SNMPv1 and SNMPv2c.

Command mode

Global configuration

Syntax

```
snmp-server enable traps snmp authentication

no snmp-server enable traps snmp authentication
```

Defaults

Generation of authentication traps is disabled

snmp targetaddr

Use this command to configure the SNMP target address. Precede this command with no to remove the configured SNMP target address.

Command mode

Global configuration

Syntax

```
snmp targetaddr <TargetAddressName> param <ParamName> {<IPAddress>
|<IP6Address>}[timeout
<Seconds(1-1500)][retries<RetryCount(1-3)][taglist <TagIdentifier |
none>][{volatile|nonvolatile}]


no snmp targetaddr <TargetAddressName>
```

Variable definitions

This table describes the variables used in the `snmp targetaddr` command.

Variable	Value
TargetAddressName	Specifies the name of the target address (host).
param	Specifies the SNMP parameter name.
IPAddress | IP6Address	Specifies the IP or IP6 address of the host.
timeout	Specifies the time the SNMP agent waits for a response from the SNMP manager before retransmitting the inform request message.
retries	Specifies the maximum number of times the agent can retransmit the inform request message.
taglist	Specifies the tag identifier.
volatile | nonvolatile	Specifies the storage type host.

Defaults

ParamName	internet
IPAddress	10.0.0.10
taglist	snmp
Storage type	volatile

Related commands

`show snmp targetaddr`

`show snmp targetparam`

`snmp targetparams`

snmp targetparams

Use this command to configure the SNMP target parameters. Precede this command with no to remove the SNMP target parameters.

Command mode

Global configuration

Syntax

```
snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c |
v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile
| nonvolatile}]


no snmp targetparams <ParamName>
```

Variable definitions

This table describes the variables used in the `snmp targetparams` command.

Variable	Value
ParamName	Specifies the SNMP target parameter name.
user	Specifies the user name.
security-model	Specifies the security model.
auth	Specifies the authentication mode. It enables Message Digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
noauth	Specifies the no authentication mode.
priv	Specifies both authentication and privacy.
message-processing	Specifies the message processing model.
volatile | nonvolatile	Specifies the storage type.

Defaults

ParamName	internet
User/Security name	none
Security model	v2c
Security level	NoauthNopriv
Message processing model	v2c
Storage type	volatile
ParamName	test1
User/Security name	none
Security model	v1
Security level	NoauthNopriv
Message processing model	v1
Storage type	volatile

Related commands

`show snmp targetparam`

`show snmp user`

`snmp user`

snmp user

Use this command to configure the SNMP user details. Precede this command with no to remove the SNMP user details.

Command mode

Global configuration

Syntax

```
snmp user <UserName> [auth {md5 | sha} <passwd> [priv DES <passwd>]]
[{volatile | nonvolatile}]


no snmp user <UserName>
```

Variable definitions

This table describes the variables used in the `snmp user` command.

Variable	Value
UserName	Specifies the user name.
auth	Specifies the authentication algorithm. It can be Message Digest 5 or Secure Hash Algorithm.
passwd	Specifies the password associated with the Authentication type.
priv DES	Specifies the private encryption password.
volatile | nonvolatile	Specifies the storage type.

Defaults

UserName	Initial
Authentication protocol	None
Privacy protocol	None
Storage type	Non-volatile

Related commands

`show snmp engineID`

`show snmp user`

snmp view

Use this command to configure the SNMP view. Precede this command with no to remove the SNMP view.

Command mode

Global configuration

Syntax

```
snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded}
[{volatile | nonvolatile}]


no snmp view <ViewName> <OIDTree>
```

Variable definitions

This table describes the variables used in the `snmp view` command.

Variable	Value
ViewName	Specifies the SNMP view name.
OIDTree	Specifies the object identifier.
OIDMask | none	Specifies the defines views' subtrees.
included | excluded	Specifies the view type.
volatile | nonvolatile	Specifies the storage type.

Defaults

ViewName	iso/restricted
OIDTree	1
OIDMask	none
ViewType	included
StorageType	non-volatile

Related commands

`show snmp group access`

`show snmp viewtree`

`snmp agent status`

snmp-server enable traps

Use this command to enable generation of a particular trap. Precede the command with no to disable generation of a particular trap.

Command mode

Global configuration

Syntax

```
snmp-server enable traps {firewall-limit | linkup | linkdown |
sip-states | sip-cfg-change | coldstart | poe-power | dhcp-pool-limit |
dsx1-line}


no snmp-server enable traps {firewall-limit | linkup | linkdown |
sip-states | sip-cfg-change | coldstart | poe-power | dhcp-pool-limit |
dsx1-line}
```

Variable definitions

This table describes the variables used in the `snmp-server enable traps` command.

Variable	Value
firewall-limit	Specifies the firewall-limit traps.
linkup	Specifies linkup traps.
linkdown	Specifies linkdown traps.
sip-states	Specifies sip-states traps.
sip-cfg-change	Specifies sip-cfg-change traps.
coldstart	Specifies coldstart traps.
poe-power	Specifies poe-power traps
dhcp-pool-limit	Specifies dhcp-pool-limit traps.
dsx1-line	Specifies dsx1-line traps.

Defaults

Generation of authentication traps is disabled

system contact

Use this command to configure the system contact information.

Command mode

Global configuration

Syntax

```
system contact <contact info>
```

Related commands

`show system information`

system location

Use this command to configure the system location.

Command mode

Global configuration

Syntax

```
system location <location name>
```

Related commands

```
show system information
```

Layer 3 commands

This section describes the command modes and commands available in Layer 3.

Layer 3 commands navigation

- Internet Protocol commands (page 384)
- Internet Group Management Protocol commands (page 411)
- Route redistribution commands (page 427)
- Virtual router redundancy protocol commands (page 436)
- Routing Information Protocol commands (page 447)
- Open Shortest Path First commands (page 467)
- Session Initiation Protocol commands (page 516)
- Linux tunnel commands (page 578)

Internet Protocol commands

Internet Protocol (IP) is an identifier for a computer or device on a Transmission Control Protocol (TCP) /IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number ranges from 0 to 255. Example: 10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random as long as each one is unique. However, to connect a private network to the Internet, the registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used to identify a particular network and a host on that network.

Four regional Internet registries (ARIN, RIPE NCC, LACNIC, and APNIC) assign Internet addresses from the following three classes:

- Class A—supports 16 million hosts on each of 126 networks
- Class B—supports 65 000 hosts on each of 16 000 networks
- Class C—supports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called Classless Inter Domain Routing (CIDR) is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.

Internet protocol commands navigation

- arp timeout (page 386)
- arp—IP address (page 387)
- ip aggregate-route (page 388)
- ip arp max-retries (page 389)
- ip default-ttl (page 390)
- ip directed-broadcast (page 391)
- ip echo-reply (page 392)
- ip mask-reply (page 393)
- ip path mtu (page 394)
- ip path mtu discover (page 395)
- ip rarp client (page 396)
- ip rarp client request (page 397)
- ip redirects (page 398)
- ip route (page 399)
- ip routing (page 400)
- ip unreachables (page 401)
- maximum-paths (page 402)
- ping (page 403)

- show ip arp (page 404)
- show ip information (page 405)
- show ip pmtu (page 406)
- show ip rarp (page 407)
- show ip traffic (page 408)
- show ip route (page 409)
- traffic-share (page 410)

arp timeout

Use this command to set the Address Resolution Protocol (ARP) cache timeout. Precede this command with no to set the ARP cache timeout to its default value.

Command mode

Global configuration

Syntax

```
arp timeout <seconds (30-86400)>


no arp timeout
```

Defaults

7200

Related commands

show ip arp

arp—IP address

Use this command to add a static entry in the ARP cache. Precede this command with no to delete a static entry from the ARP cache.

Command mode

Global configuration

Syntax

```
arp <ip address> <hardware address> {Vlan <vlan-id(1-4094)>
|<interface-type> <interface-id >} [arpa]


no arp <ip address>
```

Variable definition

This table describes the variables used in the `arp-IP address` command.

Variable	Value
ip address	Specifies the IP address or IP alias to map to the specified MAC address.
hardware address	Specifies the MAC address to map to the specified IP address or IP alias.
Vlan	Specifies the VLAN ID.
interface—type	Specifies the type of interface.
interface—id	Specifies the interface ID.
arpa	Specifies the address and routing parameter area domain.

Related commands

`show ip arp`

ip aggregate-route

Use this command to set the maximum number of aggregate routes. Precede this command with no to set the maximum number of aggregate routes to its default value.

Command mode

Global configuration

Syntax

```
ip aggregate-route <value (5-4095)>
```

```
no ip aggregate-route
```

Defaults

10

Related commands

show ip information

ip arp max-retries

Use this command to set the maximum number of ARP request retries. Precede this command with no to set the maximum number of ARP request retries to its default value.

Command mode

Global configuration

Syntax

```
ip arp max-retries <value (2-10)>


no ip arp max-retries
```

Defaults

3

Related commands

show ip arp

ip default-ttl

Use this command to set the Time To Live (TTL) value. Precede this command with no to set the TTL to the default value.

Command mode

Global configuration

Syntax

```
ip default-ttl <value (1-255)>


no ip default-ttl
```

Defaults

64 seconds

Related commands

show ip information

ip directed-broadcast

Use this command to enable forwarding of directed broadcasts. Precede this command with no to disable forwarding of directed broadcasts.

Command mode

Interface configuration

Syntax

```
ip directed-broadcast
```

```
no ip directed-broadcast
```

Defaults

Disabled

Related commands

show ip information

ip echo-reply

Use this command to enable sending ICMP echo reply messages. Precede this command with no to disable sending ICMP echo reply messages.

Command mode

Global configuration

Syntax

```
ip echo-reply
```

```
no ip echo-reply
```

Defaults

Enabled

Related commands

`show ip information`

ip mask-reply

Use this command to enable sending ICMP mask reply messages. Precede this command with no to disable sending ICMP mask reply messages.

Command mode

Global configuration

Syntax

```
ip mask-reply
```

```
no ip mask-reply
```

Defaults

Enabled

Related commands

`show ip information`

ip path mtu

Use this command to configure the MTU for usage in PMTU discovery. Precede this command with `no` to remove MTU for usage in PMTU discovery.

Command mode

Global configuration

Syntax

```
ip path mtu <dest ip> <tos> <mtu(68-65535)>


no ip path mtu <dest ip> <tos>
```

Variable definitions

This table describes the variables used in the `ip path mtu` command.

Variable	Value
dest ip	Specifies the destination IP Address.
Tos	Specifies the Type of Service (Tos) of the configured route.
Mtu	Specifies the Maximum Transmission Unit.

Related commands

`ip path mtu discover`

`show ip pmtu`

ip path mtu discover

Use this command to enable path Maximum Transmission Unit (MTU) discovery. Precede this command with no to disable path MTU discovery.

Command mode

Global configuration

Syntax

```
ip path mtu discover
```

```
no ip path mtu discover
```

Defaults

Disabled

Related commands

show ip information

ip rarp client

Use this command to enable Reverse Address Resolution Protocol (RARP) client. Precede this command with no to disable RARP client.

Command mode

Interface configuration

Syntax

```
ip rarp client
```

```
no ip rarp client
```

Defaults

Enabled

Related commands

show ip rarp

ip rarp client request

Use this command to set the number of RARP client request retries or interval between requests. Precede this command with no to set the RARP client request retries or interval between retries to their default values.

Command mode

Global configuration

Syntax

```
ip rarp client request {interval <timeout (30-3000)> | retries <retries (2-10)>}


no ip rarp client request {interval|retries}
```

Variable definitions

This table describes the variables used in the `ip rarp client request` command.

Variable	Value
interval	Specifies the interval (in seconds) after which an unanswered RARP request transmits.
retries	Specifies the maximum number of retransmissions of RARP request packet after which request must not be sent.

Defaults

interval	100
retries	4

Related commands

`show ip rarp`

ip redirects

Use this command to enable sending Internet Control Message Protocol (ICMP) redirect messages. Precede this command with no to disable sending ICMP redirect messages.

Command mode

Global configuration

Syntax

```
ip redirects
```

```
no ip redirects
```

Defaults

Enabled

Related commands

show ip information

ip route

Use this command to add a static route. Precede this command with no to delete a static route.

Command mode

Global configuration

Syntax

```
ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id (1-4094)>
|<interface-type> <interface-id>} [<distance (1-255)>]


no ip route <prefix> <mask> { <next-hop> | Vlan <vlan-id(1-4094)>
|<interface-type> <interface-id>}
```

Variable definitions

This table describes the variables used in the `ip route` command.

Variable	Value
distance	Specifies an administrative distance.
mask	Specifies the prefix mask for the destination.
next-hop	Specifies IP address or IP alias of the next hop that can be used to reach that network.
prefix	Specifies IP route prefix for the destination. (Destination IP address).
Vlan	Specifies VLAN ID.
interface-type	Specifies the type of the interface.
interface-id	Specifies the interface ID.

Defaults

distance	1

ip routing

Use this command to enable IP routing. Precede this command with no to disable IP routing.

Command mode

Global configuration

Syntax

```
ip routing
```

```
no ip routing
```

Defaults

Enabled

Related commands

show ip information

ip unreachables

Use this command to enable sending ICMP unreachable message. Precede this command with no to disable sending ICMP unreachable messages.

Command mode

Global configuration

Syntax

```
ip unreachables
```

```
no ip unreachables
```

Defaults

Enabled

Related commands

`show ip information`

maximum-paths

Use this command to set the maximum number of multipaths. Precede this command with no to set the maximum number of multipaths to its default value.

Command mode

Global configuration

Syntax

```
maximum-paths <value (1-16)>


no maximum-paths
```

Defaults

2

Related commands

show ip information

ping

Use this command to send echo messages.

Command mode

User EXEC

Syntax

```
ping [ip] destination-address [size packet_size (0-2080)] [count
packet_count (1-10)] [timeout time_out (1-100)]
```

Variable definitions

This table describes the variables used in the `ping` command.

Variable	Value
count packet_count	Specifies the number of times the given node address is to be ping.
ip	Specifies the IP address of the node to be ping.
size packet_size	Specifies the size of the data portion of the ping PDU.
timeout	Specifies the time in seconds after which the entity waiting for the ping response times out.

Defaults

size packet_size	500
count packet_count	3
timeout time_out	5

show ip arp

Use this command to display IP ARP table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip arp [{Vlan <vlan-id(1-4094)> | <ip-address> | <mac-address> |
summary | information}]
```

Variable definitions

This table describes the variables used in the `show ip arp` command.

Variable	Value
information	Specifies the ARP configuration information.
ip-address	Specifies the IP address of ARP Entry.
mac-address	Specifies the MAC address of ARP Entry.
summary	Specifies the IP ARP table summary.
Vlan	Specifies the VLAN ID.

Related commands

`arp timeout`

`arp—IP address`

`ip arp max-retries`

show ip information

Use this command to display IP configuration information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip information
```

Related commands

ip aggregate-route

ip echo-reply

ip mask-reply

ip path mtu discover

ip redirects

ip unreachables

maximum-paths

traffic-share

show ip pmtu

Use this command to display the configured PMTU Entries.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip pmtu
```

show ip rarp

Use this command to display RARP configuration information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip rarp
```

Related commands

`ip rarp client`

`ip rarp client request`

show ip traffic

Use this command to display the IP protocol statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip traffic
```

show ip route

Use this command to view the IP routing table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip route [ { <ip-address> [<mask>] | bgp | connected | ospf | rip |
static | summary } ]
```

Variable definitions

This table describes the variables used in the show `ip route` command.

Variable	Value
ip-address	Specifies destination IP address.
mask	Prefix Mask for the destination.
bgp	Specifies the Border Gateway Protocol.
connected	Displays directly connected network routes.
ospf	Specifies the Open Shortest Path First (OSPF).
rip	Specifies the Routing Information Protocol (RIP).
static	Specifies the static routes.
summary	Displays summary of all routes.

Related commands

`ip route`

`ip routing`

traffic-share

Use this command to enable traffic sharing (load sharing of IP packets). Precede this command with no to disable traffic sharing.

Command mode

Global configuration

Syntax

```
traffic-share

no traffic-share
```

Defaults

disable

Related commands

show ip information

Internet Group Management Protocol commands

Internet Group Management Protocol (IGMP) is a group membership management protocol. It helps you to report group memberships to any immediate neighboring multicast router. This protocol implements the IGMP router functionalities required by Multicast Routing Protocols (MRPs), such as PIM and Distance Vector Multicast Routing Protocol (DVMRP).

The IGMP router can be used within any routing domain that uses MRP. In addition to the group membership reports, it also informs the leave reports to MRP.

IGMP commands navigation

- debug ip igmp (page 412)
- ip igmp immediate-leave (page 413)
- ip igmp last-member-query-interval (page 414)
- ip igmp query-interval (page 415)
- ip igmp query-max-response-time (page 416)
- ip igmp robustness (page 417)
- ip igmp static-group (page 418)
- ip igmp version (page 419)
- no ip igmp (page 420)
- set ip igmp (page 421)
- show ip igmp global-config (page 422)
- show ip igmp groups (page 423)
- show ip igmp interface (page 424)
- show ip igmp sources (page 425)

debug ip igmp

Use this command to enable the IGMP trace. Precede this command with no to disable the IGMP trace.

Command mode

Privileged EXEC

Syntax

```
debug ip igmp {[i/o][grp][qry][tmr][mgmt] | [all]}

no debug ip igmp {[i/o][grp][qry][tmr][mgmt] | [all]}
```

Variable definitions

This table describes the variables used in the `debug ip igmp` command.

Variable	Value
all	Indicates all traces.
grp	Specifies group related messages.
i/o	Specifies Input/Output messages.
mgmt	Specifies management configuration messages.
qry	Specifies query related messages.
tmr	Specifies timer related messages.

Defaults

disable

ip igmp immediate-leave

Use this command to enable immediate leave processing on the interface. Precede this command with no to disable immediate-leave processing.

Command mode

Interface configuration

Syntax

```
ip igmp immediate-leave
```

```
no ip igmp immediate-leave
```

Defaults

Disabled

Related commands

show ip igmp interface

ip igmp last-member-query-interval

Use this command to set the IGMP last member query interval for the interface. Precede this command with no to set the last member query interval to the default value.

Command mode

Interface configuration

Syntax

```
ip igmp last-member-query-interval <value(1-255)>


no ip igmp last-member-query-interval
```

Defaults

10

Related commands

show ip igmp interface

ip igmp query-interval

Use this command to set the IGMP query interval for the interface. Precede this command with no to set query-interval to the default value.

Command mode

Interface configuration

Syntax

```
ip igmp query-interval <value (1-65535) seconds>


no ip igmp query-interval
```

Defaults

125

Related commands

show ip igmp interface

ip igmp query-max-response-time

Use this command to set the IGMP max query response value for the interface. Precede this command with no to set the max query response to the default value.

Command mode

Interface configuration

Syntax

```
ip igmp query-max-response-time <value (1-255) seconds>


no ip igmp query-max-response-time
```

Defaults

100

Related commands

show ip igmp interface

ip igmp robustness

Use this command to set the IGMP robustness value for the interface. Precede this command with no to set the robustness value to default value.

Command mode

Interface configuration

Syntax

```
ip igmp robustness <value(1-255)>


no ip igmp robustness
```

Defaults

2

Related commands

show ip igmp interface

ip igmp static-group

Use this command to the static group membership on the interface. Precede this command with no to delete the static group membership on the interface.

Command mode

Interface configuration

Syntax

```
ip igmp static-group <Group Address> [source <Source Address>]

no ip igmp static-group <Group Address> [source <Source Address>]
```

Variable definitions

This table describes the variables used in the `ip igmp static-group` command.

Variable	Value
Group Address	Specifies the group IP address.
source	Specifies the source IP address.

Related commands

`show ip igmp groups`

`show ip igmp interface`

`show ip igmp sources`

ip igmp version

Use this command to set the IGMP version on the interface. Precede this command with no to set the default IGMP version on the interface.

Command mode

Interface configuration

Syntax

```
ip igmp version {1 | 2 | 3}
```

```
no ip igmp version
```

Defaults

2

Related commands

show ip igmp interface

no ip igmp

Use this command to delete the IGMP capable interface.

Command mode

Interface configuration

Syntax

```
no ip igmp
```

Related commands

`show ip igmp interface`

set ip igmp

Use this command to enable or disable IGMP on the interface.

Command mode

Global configuration or Interface configuration

Syntax

```
set ip igmp {enable | disable}
```

Variable definitions

This table describes the variables used in the **`set ip igmp`** command.

Variable	Value
disable	Disables IGMP.
enable	Enables IGMP.

Defaults

Disabled

Related commands

`show ip igmp global-config`

`show ip igmp interface`

show ip igmp global-config

Use this command to display the global configuration of IGMP.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp global-config
```

Related commands

`set ip igmp`

show ip igmp groups

Use this command to display the IGMP groups information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp groups
```

Related commands

`ip igmp static-group`

show ip igmp interface

Use this command to display the interface configuration of IGMP.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp interface [Vlan <vlan-id>]
```

Variable definitions

This table describes the variables used in the `show ip igmp interface` command.

Variable	Value
Vlan	Specifies VLAN ID.

Related commands

`ip igmp immediate-leave`

`ip igmp last-member-query-interval`

`ip igmp query-interval`

`ip igmp query-max-response-time`

`ip igmp robustness`

`ip igmp version`

`no ip igmp`

`set ip igmp`

show ip igmp sources

Use this command to display the IGMP source information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp sources
```

Related commands

`ip igmp static-group`

show ip igmp statistics

Use this command to view the IGMP statistics information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip igmp statistics [Vlan <vlan-id>]
```

Route redistribution commands

Route redistribution (RRD) allows different routing protocols to exchange routing information. Redistribution uses a routing protocol to advertise routes that are learned by other means such as another routing protocol, static routes, or directly connected routes. Running a single routing protocol throughout an entire IP internetwork is efficient, but multi-protocol routing is often used. For example, when a company merges, multiple departments are managed by multiple network administrators. If a single routing protocol cannot be used, route redistribution is the only solution.

Each routing protocol on a network is separated into an autonomous system (AS). All routers in the same autonomous system (running the same routing protocol) have complete knowledge of the entire autonomous system. A router that connects two (or more) autonomous systems is known as a border router. A border router advertises routing information from one autonomous system to the other autonomous systems. You can only redistribute routing information for like routed protocols. Different routing protocols have different, and often incompatible, algorithms and metrics.

RRD navigation

- as-num (page 428)
- default redistribute-policy (page 429)
- export ospf (page 430)
- redistribute-policy (page 431)
- router-id (page 432)
- show ip protocols (page 433)
- show redistribute information (page 434)
- show redistribute-policy (page 435)

as-num

Use this command to set the AS number for the router.

Command mode

Global configuration

Syntax

```
as-num <value(1-65535)>
```

Defaults

0

Related commands

`show redistribute information`

default redistribute-policy

Use this command to set the default behavior of RRD control table.

Command mode

Global configuration

Syntax

```
default redistribute-policy {permit | deny}
```

Variable definitions

This table describes the variables used in the `dot1x control-direction` command.

Variable	Value
deny	Sets the default rule for all prefixes to deny.
permit	Sets the default rule for all prefixes to permit.

Related commands

`show redistribute-policy`

export ospf

Use this command to enable redistribution of Open Shortest Path First (OSPF) area or external routes to the protocol. Precede this command with no to disable redistribution of OSPF area or external routes to the protocol.

Command mode

Global configuration

Syntax

```
export ospf {area-route | external-route} {rip|bgp}


no export ospf {area-route|external-route} {rip|bgp}
```

Variable definitions

This table describes the variables used in the `export ospf` command.

Variable	Value
area-route	Specifies the OSPF inter-area and intra-area address or mask pairs to be exported into the routing protocol.
bgp	Specifies border gateway protocol.
external-route	Specifies the OSPF type 1 and type 2 external address or mask pairs to be exported into the routing protocol.
rip	Specifies routing information protocol.

Related commands

`show ip protocols`

redistribute-policy

Use this command to add the permit or deny redistribution policy. Precede this command with no to remove the permit or deny redistribution policy.

Command mode

Global configuration

Syntax

```
redistribute-policy {permit | deny}  <DestIp> <DestRange> {static | rip |
ospf | bgp}  {rip | bgp | ospf | all}


no redistribute-policy <DestIp> <DestRange>
```

Variable definitions

This table describes the variables used in the `redistribute-policy` command.

Variable	Value
all	Indicates all distribution policy.
bgp	Specifies border gateway protocol.
deny	Sets the default rule for all prefixes to deny.
DestIp	Specifies destination IP address.
DestRange	Specifies destination range.
ospf	Specifies open shortest path first.
permit	Sets the default rule for all prefixes to permit.
rip	Routing information protocol.
static	Indicates static routes.

Defaults

Permit all

Related commands

`show redistribute-policy`

router-id

Use this command to set the ID address for the router.

Command mode

Global configuration

Syntax

```
router-id <addr>
```

Related commands

`show redistribute information`

show ip protocols

Use this command to display information about the active routing protocol process.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip protocols
```

Related commands

`export ospf`

show redistribute information

Use this command to display Route Table Manager (RTM) RRD status for registered protocols.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show redistribute information
```

Related commands

as-num

router-id

show redistribute-policy

Use this command to display route redistribution filters.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show redistribute-policy
```

Related commands

`redistribute-policy`

`default redistribute-policy`

Virtual router redundancy protocol commands

Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN. This allows several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router. VRRP eliminates the single point of failure inherent in the static default routed environment.

VRRP navigation

- debug VRRP (page 437)
- interface vlan (page 438)
- router vrrp (page 439)
- show vrrp —vrid (page 440)
- show vrrp interface vlan (page 441)
- vrrp-interval (page 442)
- vrrp-ip address (page 443)
- vrrp—preempt (page 444)
- vrrp—priority (page 445)
- vrrp - text-authentication (page 446)

debug VRRP

Use this command to enable the trace for the VRRP module. Precede this command with no to disable the trace for VRRP module.

Command mode

Privileged EXEC

Syntax

```
debug VRRP
```

```
no debug VRRP
```

Defaults

Debugging is disabled

interface vlan

Use this command to select an interface to configure. Precede this command with no to delete the virtual router entries on the given interface.

Command mode

VRRP router configuration

Syntax

```
interface vlan <vlan-id (1-4094)>


no interface Vlan <vlan-id (1-4094)>
```

Variable definitions

This table describes the variables used in the `interface vlan` command.

Variable	Value
vlan-id	Specifies VLAN identifier.

Related commands

`router vrrp`

`show vrrp –vrid`

router vrrp

Use this command to enable VRRP in the router and is used to enter the VRRP configuration mode. Precede this command with no to disable VRRP in the router.

Command mode

Global configuration

Syntax

```
router vrrp
```

```
no router vrrp
```

Defaults

VRRP is disabled

Related commands

show vrrp —vrid

show vrrp —vrid

Use this command to display the VRRP status information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vrrp [interface vlan <VlanId(1-4094)> <VrId(1-255)>] [{brief |
detail |statistics}]
```

Variable definitions

This table describes the variables used in the `show vrrp—vrid` command.

Variable	Value
interface vlan	VRRP information on the given VLAN ID and VRID.
brief	Displays information about VRRP in brief.
detail	Displays information about VRRP in detail.
statistics	Displays VRRP statistics.

Related commands

`interface vlan`

`router vrrp`

`vrrp-ip address`

show vrrp interface vlan

Use this command to display the VRRP status information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vrrp [interface vlan <VlanId(1-4094)> ] [{brief | detail
|statistics}]
```

Variable definitions

This table describes the variables used in the `show vrrp interface vlan` command.

Variable	Value
interface vlan	VRRP information on the given VLAN ID.
brief	Displays information about VRRP in brief.
detail	Displays information about VRRP in detail.
statistics	Displays VRRP statistics.

Related commands

`interface vlan`

`router vrrp`

`vrrp-ip address`

vrrp-interval

Use this command to set the advertisement timer for a virtual router. Precede this command with no to set the advertisement timer for a virtual router to default value.

Command mode

VRRP interface configuration

Syntax

```
vrrp <vrid(1-255)> timer <interval(1-255)secs>


no vrrp <vrid(1-255)> timer
```

Variable definitions

This table describes the variables used in the **vrrp-interval** command.

Variable	Value
timer	Specifies the time interval, in seconds, between sending advertisement messages.
vrid	Specifies the Virtual router ID.

Defaults

1 second

Related commands

router vrrp

show vrrp –vrid

vrrp-ip address

Use this command to set the associated IP addresses for the virtual router. Precede this command with no to delete the associated IP addresses for the virtual router.

Command mode

VRRP interface configuration

Syntax

```
vrrp <vrid(1-255)> ipv4 <ucast_addr>
```

no vrrp <vrid(1-255)> ipv4 [<ucast_addr>]

Variable definitions

This table describes the variables used in the `vrrp-ip address` command.

Variable	Value
ipv4	Specifies the IP address.
vrid	Specifies the Virtual router ID.

Related commands

`router vrrp`

`show vrrp –vrid`

vrrp—preempt

Use this command to enable the preemption of state change from either backup to master or vice versa based on the election process. Precede this command with no to disable the preempt mode.

Command mode

VRRP interface configuration

Syntax

```
vrrp <vrid(1-255)> preempt


no vrrp <vrid(1-255)> preempt
```

Variable definitions

This table describes the variables used in the `vrrp-preempt` command.

Variable	Value
preempt	Enables preemption of VRRP router states.
vrid	Specifies the virtual router ID.

Defaults

Preemption is enabled

Related commands

`router vrrp`

`show vrrp –vrid`

vrrp—priority

Use this command to set the priority for the virtual router. Precede this command with no to set the priority for the virtual router to default value.

Command mode

VRRP interface configuration

Syntax

```
vrrp <vrid(1-255)> priority <priority(1-255)>


no vrrp <vrid(1-255)> priority
```

Variable definitions

This table describes the variables used in the `vrrp—priority` command.

Variable	Value
priority	Specifies the priority used for the virtual router master election process.
vrid	Speicfies virtual router ID.

Defaults

100

Related commands

`router vrrp`

`show vrrp –vrid`

vrrp - text-authentication

Use this command to set the authentication type for the virtual router to simple password. Precede this command with no to set the authentication type for the virtual router to none.

Command mode

VRRP interface configuration

Syntax

```
vrrp <vrid(1-255)> text-authentication <password>


no vrrp <vrid(1-255)> text-authentication
```

Variable definitions

This table describes the variables used in the `vrrp - text-authentication` command.

Variable	Value
text-authentication	Indicates authentication password.
vrid	Specifies virtual router ID.

Related commands

`router vrrp`

`show vrrp –vrid`

Routing Information Protocol commands

Routing Information Protocol (RIP) is a widely used protocol for managing router information within a self-contained network such as a corporate Local Area Network (LAN) or an interconnected group of such LANs. RIP is classified by the Internet Engineering Task Force (IETF) as one of several Internal Gateway Protocols (IGP).

RIP sends routing update messages at regular intervals and also when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is identified as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

RIP navigation

- auto-summary (page 448)
- debug ip rip (page 449)
- default-metric (page 450)
- ip rip authentication mode (page 451)
- ip rip default route originate (page 452)
- ip rip receive version (page 453)
- ip rip retransmission (page 454)
- ip rip security (page 455)
- ip rip send version (page 456)
- ip rip summary-address (page 457)
- ip spilt-horizon (page 458)
- neighbor (page 459)
- network (page 460)
- output-delay (page 461)
- passive-interface vlan (page 462)
- redistribute (page 463)
- router rip (page 464)
- show ip rip (page 465)
- timers basic (page 466)

auto-summary

Use this command to enable or to disable the auto summarization feature in RIP.

Command mode

Router configuration

Syntax

```
auto-summary {enable | disable}
```

Variable definitions

This table describes the variables used in the `auto-summary` command.

Variable	Value
enable	Enables auto summarization feature in RIP.
disable	Disables auto summarization feature in RIP.

Defaults

Enable

Related commands

`show ip rip`

debug ip rip

Use this command to set the debug level for RIP module. Precede this command with no to reset the debug level for RIP module.

Command mode

Privileged EXEC

Syntax

```
debug ip rip {all | init | data | control | dump | os | mgmt | failure |
buffer}
```

```
no debug ip rip { all | init | data | control | dump | os | mgmt |
failure | buffer }
```

Variable definitions

This table describes the variables used in the `debug ip rip` command.

Variable	Value
all	Specifies all resources.
buffer	Specifies buffer messages.
control	Specifies control plane messages.
data	Specifies data path messages.
dump	Specifies packet dump messages.
failure	Specifies all failure messages (including packet validation).
init	Specifies initialization and shutdown messages.
mgmt	Specifies management messages.
os	Specifies OS resource messages.

Defaults

init

Related commands

`show ip rip`

default-metric

Use this command to set the RIP default metric. Precede this command with no to set the RIP metric to its default value.

Command mode

Router configuration

Syntax

```
default-metric <value>


no default-metric
```

Defaults

3

Related commands

redistribute

show ip rip

ip rip authentication mode

Use this command to configure authentication mode and key. Precede this command with no to disable authentication.

Command mode

Interface configuration

Syntax

```
ip rip authentication mode {text | md5 } key-chain <key-chain-name (16)>

no ip rip authentication
```

Variable definitions

This table describes the variables used in the `ip rip authentication mode` command.

Variable	Value
key-chain	Specifies the authentication key value.
md5	Indicates key Message Digest 5 (MD5) authentication. More than one entry can be configured for an interface.
text	Clears text authentication.

Defaults

No authentication

Related commands

`show ip rip`

ip rip default route originate

Use this command to configure the metric to be used for default route propagated over the interface. Precede this command with `no` to disable the origin of default route over the interface.

Command mode

Interface configuration

Syntax

```
ip rip default route originate <metric(1-15)>


no ip rip default route originate
```

Variable definitions

This table describes the variables used in the `ip rip default route originate` command.

Variable	Value
metric	Specifies the value for the metric.

Defaults

no ip rip default route originates

Related commands

`show ip rip`

ip rip receive version

Use this command to set IP RIP version number for receiving advertisements. Precede this command with no to set IP RIP receive version number to its default value.

Command mode

Interface configuration

Syntax

```
ip rip receive version  {1 | 2 | 1 2 | none}
```

```
no ip rip receive version
```

Variable definitions

This table describes the variables used in the `ip rip receive version` command.

Variable	Value
1 | 2 | 1 2 | none	Indicates which version of RIP updates are accepted.

Defaults

1 2

Related commands

`ip rip send version`

`show ip rip`

ip rip retransmission

Use this command to configure the timeout interval. Insert the number of retries to retransmit the update request packet or an unacknowledged update response packet. Precede this command with no to set the retransmission timeout interval or the number of retransmission retries to its default value.

Command mode

Router configuration

Syntax

```
ip rip retransmission {interval <timeout-value (5-10)> | retries <value (10-40)>}


no ip rip retransmit {interval | retries}
```

Variable definitions

This table describes the variables used in the `ip rip retransmission` command.

Variable	Value
interval	Specifies the timeout interval to be used to retransmit the update request packet or an unacknowledged update response packet.
retries	Specifies the maximum number of retransmissions of the update request and update response packets.

Defaults

interval	5
retries	36

Related commands

`show ip rip`

ip rip security

Use this command to accept or ignore RIP1 packets when authentication is in use. Precede this command with no to the security level to its default value.

Command mode

Router configuration

Syntax

```
ip rip security {minimum | maximum}
```

```
no ip rip security
```

Variable definitions

This table describes the variables used in the `ip rip security` command.

Variable	Value
minimum	Denotes that the RIP1 packets will be accepted even when authentication is in use.
maximum	Denotes that RIP1 packets will be ignored when authentication is in use.

Defaults

maximum

Related commands

`show ip rip`

ip rip send version

Use this command to set the IP RIP version number for transmitting advertisements. Precede this command with no to set IP RIP send version number to its default value.

Command mode

Interface configuration

Syntax

```
ip rip send version  {1 | 2 | 1 2 | none}
```

```
no ip rip send version
```

Variable definitions

This table describes the variables used in the `ip rip send version` command.

Variable	Value
1 | 2 | 1 2 | none	Indicates which version of RIP updates are sent.

Defaults

1 2

Related commands

`ip rip receive version`

`show ip rip`

ip rip summary-address

Use this command to command route aggregation for all subnet routes that falls under the specified IP address and mask. Precede the command with `no` form to disable route aggregation with the specified IP address and mask.

Command mode

Interface configuration

Syntax

```
ip rip summary-address <ip-address> <mask>
```

```
no ip rip summary-address <ip-address> <mask>
```

Variable definitions

This table describes the variables used in the `ip rip summary-address` command.

Variable	Value
ip-address	Specifies the IP Address of the interface specific aggregation.
mask	Specifies the subnet mask.

Related commands

`show ip protocols`

ip spilt-horizon

Use this command to set the spilt horizon status. Precede this command with no to disable the spilt horizon status.

Command mode

Interface configuration

Syntax

```
ip spilt-horizon [poisson]


no ip spilt-horizon
```

Variable definitions

This table describes the variables used in the `ip split-horizon` command.

Variable	Value
poisson	Splits horizon with poisson method enabled.

Related commands

`show ip rip`

neighbor

Use this command to add a neighbor router and to set its priority. Precede this command with no to delete a neighbor router or to set default value for the neighbor priority.

Command mode

Router configuration

Syntax

```
neighbor <neighbor-id> [priority  <priority value (0-255)>]

no neighbor <neighbor-id> [priority]
```

Variable definitions

This table describes the variables used in the `neighbor` command.

Variable	Value
neighbor-id	Specifies the neighbor id value to add a router.
priority	Specifies a number value that specifies the router priority.

Defaults

priority	1

Related commands

`ip ospf priority`

`ip ospf network`

`show ip ospf neighbor`

network

Use this command to enable RIP on an IP network. Precede this command with no to disable RIP on an IP network.

Command mode

Router configuration

Syntax

```
network <ip-address>


no network <ip-address>
```

Variable definitions

This table describes the variables used in the network command.

Variable	Value
ip-address	Specifies the IP address for the entry.

Related commands

router rip

show ip rip

output-delay

Use this command to enable interpacket delay for RIP updates. Precede this command with no to disable interpacket delay for RIP updates.

Command mode

Router configuration

Syntax

```
output-delay


no output-delay
```

Related commands

show ip rip

passive-interface vlan

Use this command to suppress routing updates on an interface. Precede this command with no to not suppress routing updates on an interface.

Command mode

Router configuration

Syntax

```
passive-interface vlan <vlan-id(1-4094)>


no passive-interface vlan <vlan-id(1-4094)>
```

Related commands

show ip rip

redistribute

Use this command to enable redistribution of corresponding protocol routes into RIP. Precede this command with no to disable redistribution of corresponding protocol routes into RIP.

Command mode

Router configuration

Syntax

```
redistribute {all | bgp | connected | ospf | static}

no redistribute {all | bgp | connected | ospf | static}
```

Variable definitions

This table describes the variables used in the `redistribute` command.

Variable	Value
all	Advertises all routes learned in the RIP process.
bgp	Advertises routes learned by BGP in the RIP process.
connected	Indicates connected routes redistribution.
ospf	Advertises routes learned by OSPF in the RIP process.
static	Indicates statically configured routes to advertise in the RIP process.

Related commands

`default-metric`

`show ip rip`

router rip

Use this command to enter the router configuration mode. Precede this command with no to disable RIP on all the interfaces.

Command mode

Global configuration

Syntax

```
router rip
```

```
no router rip
```

Related commands

network

show ip rip

show ip rip

Use this command to IP RIP protocol database or statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip rip {database [<ip-address> <ip-mask>] | statistics}
```

Variable definitions

This table describes the variables used in the `show ip rip` command.

Variable	Value
database	Specifies the RIP protocol database for the specified IP address and IP mask of the RIP interface entry.
statistics	Specifies the RIP statistics on the router.

Related commands

`debug ip rip`

`default-metric`

`ip rip authentication mode`

`ip rip receive version`

`ip rip retransmission`

`ip rip security`

`ip rip send version`

`ip spilt-horizon`

`neighbor`

`network`

`output-delay`

`passive-interface vlan`

`redistribute`

`router rip`

`timers basic`

timers basic

Use this command to set update, route age, and garbage collection timers. Precede this command with `no` to set update, route age, and garbage collection timers to the default values.

Command mode

Interface configuration

Syntax

```
timers basic <update-value (10-3600)> <routeage-value (30-500)>
<garbage-value (120-180)>


no timers basic
```

Variable definitions

This table describes the variables used in the `timers basic` command.

Variable	Value
garbage-value	Specifies time after which the entry is put into garbage collect interval.
routeage-value	Specifies interval before deleting an entry after not hearing it.
update-value	Specifies interval time between updates.

Defaults

garbage-value	120
routeage-value	180
update-value	30

Related commands

`show ip rip`

Open Shortest Path First commands

Open Shortest Path First (OSPF) protocol is an Interior Gateway Protocol (IGP) used for distributing routing information within a single AS. Routers use link state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the internet constructed by each node. Each router sends that portion of the routing table (it keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller, more frequent updates. They converge quickly, thus preventing such problems as routing loops and count-to-infinity (when routers continuously increment the hop count to a particular network), resulting in a stable network.

All OSPF interface-related configurations are done when the global OSPF is enabled.

OSPF commands navigation

- abr-type (page 469)
- area—default cost (page 470)
- area—nssa (page 471)
- area—range (page 472)
- area—stability-interval (page 474)
- area—stub (page 475)
- area—translation-role (page 476)
- area—virtual-link (page 477)
- ASBR Router (page 479)
- compatible rfc1583 (page 480)
- debug ip ospf (page 481)
- default-information originate always (page 482)
- ip ospf authentication (page 483)
- ip ospf authentication-key (page 484)
- ip ospf cost (page 485)
- ip ospf dead-interval (page 486)
- ip ospf demand-circuit (page 487)
- ip ospf hello-interval (page 488)
- ip ospf message-digest-key (page 489)
- ip ospf network (page 490)
- ip ospf priority (page 491)
- ip ospf retransmit-interval (page 492)
- ip ospf transmit-delay (page 493)
- neighbor (page 494)
- network (page 495)

- passive-interface default (page 496)
- passive-interface vlan (page 497)
- redistribute (page 498)
- redist-config (page 499)
- router-id (page 500)
- router ospf (page 501)
- set nssa asbr-default-route translator (page 502)
- show ip ospf (page 503)
- show ip ospf border-routers (page 504)
- show ip ospf—database (page 505)
- show ip ospf—database summary (page 506)
- show ip ospf interface (page 507)
- show ip ospf neighbor (page 508)
- show ip ospf request-list (page 509)
- show ip ospf retransmission-list (page 510)
- show ip ospf route (page 511)
- show ip ospf—summary address (page 512)
- show ip ospf virtual-links (page 513)
- summary-address (page 514)

abr-type

Use this command to set the alternative ABR Type.

Command mode

Router configuration

Syntax

```
abr-type {standard | cisco | ibm}
```

Variable definitions

This table describes the variables used in the `abr-type` command.

Variable	Value
cisco	Specifies CISCO ABR type as defined in RFC 3509.
ibm	Specifies IBM ABR type as defined in RFC 3509.
standard	Specifies standard ABR type as defined in RFC 2328.

Defaults

Standard

Related commands

`router ospf`

`show ip ospf`

area—default cost

Use this command to specify a cost for the default summary route sent into a stub or NSSA. Precede this command with no to remove the assigned default route cost.

Command mode

Router configuration

Syntax

```
area <area-id> default-cost <cost> [tos <tos value(0-30)>]


no area <area-id> default-cost [tos <tos value (0-30)>]
```

Variable definitions

This table describes the variables used in the `area—default cost` command.

Variable	Value
area-id	Specifies area associated with the OSPF address range. It is specified as an IP address.
default-cost	Specifies the cost for the default summary route used for a stub area.
tos	Specifies the type of service of the route being configured.

Defaults

default-cost	10
tos	0

Related commands

area—range

area—stub

ip ospf authentication

ip ospf cost

area—nssa

Use this command to configure an area as a NSSA and other parameters related to that area.

Command mode

Router configuration

Syntax

```
area <area-id> nssa [{no-summary | default-information-originate [metric
<value>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>]}]
```

Variable definitions

This table describes the variables used in the `area—nssa` command.

Variable	Value
area-id	Specifies area associated with the OSPF address range. It is specified as an IP address.
default-information-originate	Specifies default route into OSPF metric— The metric value applied to the route before it is advertised. into the OSPF domain. metric-type —The metric type applied to the route before it is advertised. into the OSPF domain. tos— type of service of the route being configured.
no-summary	Indicates allows an area to be a not-so-stubby area but not have summary routes injected into it.
nssa	Configures an area as a not-so-stubby area (NSSA).

Defaults

metric	10
metric-type	1
tos	0

Related commands

`area—range`

`area—translation-role`

area—range

Use this command to consolidate and summarize routes at an area boundary. Precede this command with no to delete the summary address.

Command mode

Router configuration

Syntax

```
area <AreaId> range <Network> <Mask> {summary | Type7} [{advertise |
not-advertise}] [tag <value>]


no area <AreaId> range <Network> <Mask>
```

Variable definitions

This table describes the variables used in the `area—range` command.

Variable	Value
advertise	When set to advertise and associated area Id is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated area Id is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x.
AreaId	Area associated with the OSPF address range. It is specified as an IP address.
Mask	Specifies the subnet mask that pertains to the range.
Network	Specifies the IP address of the Net indicated by the range.
not-advertise	When set to doNotAdvertise (2) and associated areaId is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if associated areaId is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range.
range	Specifies OSPF address range.
summary	Indicates summary LSAs.
tag	The Tag type describes whether tags will be automatically generated or will be manually configured.
Type7	Indicates type-7 LSA.

Defaults

tag	2

Related commands

area—default cost

area—nssa

area—stub

area—virtual-link

ip ospf authentication

show ip ospf—summary address

summary-address

area—stability-interval

Use this command to configure the stability interval for Not So Stubby Area (NSSA). Precede this command with no to configure default stability interval for NSSA.

Command mode

Router configuration

Syntax

```
area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>


no area <area-id> stability-interval
```

Variable definitions

This table describes the variables used in the `area—stability-interval` command.

Variable	Value
area-id	Specifies area associated with the OSPF address range. It is specified as an IP address.
stability-interval	Specifies the number of seconds after an elected translator determines its services are no longer required, that it must continue to perform its translation duties.

Defaults

40

Related commands

`show ip ospf`

area—stub

Use this command to an area as a stub area and other parameters related to that area. Precede this command with no to remove an area or convert stub or nssa to normal area.

Command mode

Router configuration

Syntax

```
area <area-id> stub [no-summary]
no area <area-id> [{ stub | nssa }]
```

Variable definitions

This table describes the variables used in the area—stub command.

Variable	Value
area-id	Specifies area associated with the OSPF address range. It is specified as an IP address.
stub	Specifies stub area. If the area type is no-summary, the router will neither originate nor propagate summary LSAs into the stub area.
no-summary	If specified, router neither originates nor propogates summary LSAs into the stub area.
nssa	Specifies not-so-stubby area.

Related commands

area—default cost

area—range

ip ospf authentication

area—translation-role

Use this command to configure the translation role for NSSA. Precede this command with no to configure default translation role for NSSA.

Command mode

Router configuration

Syntax

```
area  <area-id> translation-role {always | candidate}

no area  <area-id> translation-role
```

Variable definitions

This table describes the variables used in the area—translation-role command.

Variable	Value
area-id	Specifies the area associated with the OSPF address range. It is specified as an IP address.
translation-role	Specifies a NSSA border router's ability to perform NSSA translation of Type-7 LSAs to Type-5 LSAs.

Defaults

candidate

Related commands

area—nssa

area—virtual-link

Use this command to an OSPF virtual link and its related parameters. Precede this command with no to remove an OSPF virtual link.

Command mode

Router configuration

Syntax

```
area <area-id> virtual-link <router-id> [authentication {message-digest
| null}] [hello-interval <value (1-65535)>] [retransmit-interval <value
(0-3600)>] [transmit-delay <value (0-3600)>] [dead-interval <value>]
[{authentication-key <key (8)> | message-digest-key <Key-id (0-255)> md5
<key (16)>}]
```

```
no area <area-id> virtual-link <router-id> [authentication]
[hello-interval] [retransmit-interval] [transmit-delay] [dead-interval]
[{authentication-key | message-digest-key <Key-id (0-255)>}]
```

Variable definitions

This table describes the variables used in the `area-virtual-link` command.

Variable	Value
area-id	Specifies the transit area that the virtual link traverses. It is specified as an IP address.
authentication	Indicates the authentication type for an interface.
authentication-key	Identifies the secret key used to create the message digest appended to the OSPF packet.
dead-interval	Specifies the interval at which hello packets must not be seen before its neighbors declare the router down (the range of values for the dead interval is 0-0x7fffffff).
hello-interval	The interval between hello packets that the software sends on the OSPF virtual link interface.
md5	The secret key which is used to create the message digest appended to the OSPF packet.
message-digest-key	Specifies OSPF MD5 authentication. Enables Message Digest 5 (MD5) authentication on the area specified by the area-id.
retransmit-interval	Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface.

Variable	Value
transmit-delay	Specifies the time the router will stop using this key for packets generation.
virtual-link	Specifies the router ID of the virtual neighbor.

Defaults

authentication	null
hello-interval	10
retransmit-interval	5
transmit-delay	1
dead-interval	40

Related commands

area—range

ip ospf authentication

show ip ospf

show ip ospf virtual-links

ASBR Router

Use this command to specify this router as ASBR. Precede this command with no to disable this router as ASBR.

Command mode

Router configuration

Syntax

```
ASBR Router


no ASBR Router
```

Related commands

`set nssa asbr-default-route translator`

`show ip ospf`

compatible rfc1583

Use this command to set OSPF compatibility list compatible with RFC 1583. Precede this command with no to disable RFC 1583 compatibility.

Command mode

Router configuration

Syntax

```
compatible rfc1583


no compatible rfc1583
```

Defaults

Enabled

Related commands

show ip ospf

debug ip ospf

Use this command to set the OSPF debug level. Precede this command with no to remove an old MD5 key.

Command mode

Privileged EXEC

Syntax

```
debug ip ospf {pkt  {hp | ddp | lrq | lsu | lsa }  | module
{adj_formation | ism | nsm | config | interface }  }
```

```
no debug ip ospf { pkt  {hp | ddp | lrq | lsu | lsa }  | module
{adj_formation | ism | nsm | config | interface} | all }
```

Variable definitions

This table describes the variables used in the `debug ip ospf` command.

Variable	Value
adj_formation	Specifies adjacency formation debug messages.
config	Specifies configuration debug messages.
ddp	Specifies DDP packet debug messages.
hp	Specifies hello packet debug messages.
interface	Specifies interface.
ism	Specifies the interface state machine debug messages.
lrq	Link state request packet debug messages.
lsa	Link state acknowledge packet debug messages.
lsu	Link state update packet debug messages.
module	RTM module debug messages.
nsm	Neighbor state machine debug messages.
pkt	Specifies packet high level dump debug messages.

Related commands

`show ip ospf`

default-information originate always

Use this command to enable generation of a default external route into an OSPF routing domain and other parameters related to that area. Precede this command with no to disable generation of a default external route into an OSPF routing domain.

Command mode

Router configuration

Syntax

```
default-information originate always [metric <metric-value
(0-0xffffff)>] [metric-type <type (1-2)>]


no default-information originate always [metric <metric-value
(0-0xffffff)>] [metric-type <type (1-2)>]
```

Variable definitions

This table describes the variables used in the `default-information originate always` command.

Variable	Value
metric	Specifies the metric value applied to the route before it is advertised into the OSPF domain.
metric-type	Specifies the metric type applied to the route before it is advertised into the OSPF domain.

Defaults

metric	10
metric-type	2

Related commands

`redistribute`

ip ospf authentication

Use this command to specify a password authentication type for an interface. Precede this command with no to remove the authentication type for an interface and set it to NULL authentication.

Command mode

Interface configuration

Syntax

```
ip ospf authentication [{message-digest | null}]


no ip ospf authentication
```

Variable definitions

This table describes the variables used in the `ip ospf authentication` command.

Variable	Value
message-digest	Specifies message digest authentication.
null	Indicates NULL authentication.

Defaults

null

Related commands

`area–default cost`

`area–range`

`area–stub`

`area–virtual-link`

`ip ospf authentication-key`

`ip ospf message-digest-key`

ip ospf authentication-key

Use this command to specify a password for the neighboring routers that are using the OSPF simple password authentication. Precede this command with no to remove any existing assigned OSPF password.

Command mode

Interface configuration

Syntax

```
ip ospf authentication-key <password (8)>


no ip ospf authentication-key
```

Related commands

ip ospf authentication

show ip ospf

summary-address

ip ospf cost

Use this command to specify the cost of sending a packet on an interface. Precede this command with no to reset the path cost to the default value.

Command mode

Interface configuration

Syntax

```
ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]


no ip ospf cost [tos <tos value (0-30)>]
```

Variable definitions

This table describes the variables used in the `ip ospf cost` command.

Variable	Value
cost	Specifies the type 1 external metrics which is expressed in the same units as OSPF interface cost, that is in terms of the OSPF link state metric.
tos	Specifies the type of service (tos) of the route being configured.

Defaults

0

Related commands

`area—default cost`

`show ip ospf interface`

ip ospf dead-interval

Use this command to set the interval at which hello packets must not be seen before neighbors declare the router down. Precede this command with no to set the default value for the interval at which hello packets must not be seen before neighbors declare the router down.

Command mode

Interface configuration

Syntax

```
ip ospf dead-interval <seconds (0-0x7fffffff)>


no ip ospf dead-interval
```

Defaults

40

Related commands

ip ospf hello-interval

ip ospf retransmit-interval

ip ospf transmit-delay

show ip ospf interface

ip ospf demand-circuit

Use this command to configure the OSPF to treat the interface as an OSPF demand circuit. Precede this command with no to remove the demand circuit designation from the interface.

Command mode

Interface configuration

Syntax

```
ip ospf demand-circuit
```

```
no ip ospf demand-circuit
```

Related commands

show ip ospf interface

ip ospf hello-interval

Use this command to specify the interval between hello packets sent on the interface. Precede this command with no to set the default value for the interval between hello packets sent on the interface.

Command mode

Interface configuration

Syntax

```
ip ospf hello-interval <seconds (1 - 65535)>


no ip ospf hello-interval
```

Defaults

10

Related commands

ip ospf dead-interval

ip ospf retransmit-interval

ip ospf transmit-delay

show ip ospf interface

ip ospf message-digest-key

Use this command to enable OSPF MD5 authentication. Precede this command with no to remove an old MD5 key.

Command mode

Interface configuration

Syntax

```
ip ospf message-digest-key <Key-ID (0-255)> md5 <md5-Key (16)>

no ip ospf message-digest-key <Key-ID (0-255)>
```

Variable definitions

This table describes the variables used in the `ip ospf message-digest-key` command.

Variable	Value
Key-ID	Identifies the secret key, which is used to create the message digest appended to the OSPF packet.
md5	Specifies the secret key, which is used to create the message digest appended to the OSPF packet.

Related commands

`ip ospf authentication`

`summary-address`

`show ip ospf`

ip ospf network

Use this command to configure the OSPF network type to a type other than the default for a given media. Precede this command with no to set the OSPF network type to the default type.

Command mode

Interface configuration

Syntax

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint |
point-to-point}


no ip ospf network
```

Variable definitions

This table describes the variables used in the `ip ospf network` command.

Variable	Value
broadcast	Specifies the networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast).
non-broadcast	Specifies the networks supporting many (more than two) routers, but having no broadcast capability.
point-to-multipoint	Treats the non-broadcast network as a collection of point-to-point links.
point-to-point	Specifies a network that joins a single pair of routers.

Related commands

`ip ospf priority`

`neighbor`

`show ip ospf interface`

ip ospf priority

Use this command to configure the router priority. Precede this command with no to set default value for router priority.

Command mode

Interface configuration

Syntax

```
ip ospf priority <value (0 - 255)>


no ip ospf priority
```

Defaults

1

Related commands

ip ospf network

neighbor

ip ospf retransmit-interval

Use this command to specify the time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Precede this command with no to use the default time between LSA retransmissions for adjacencies belonging to the interface.

Command mode

Interface configuration

Syntax

```
ip ospf retransmit-interval <seconds (0 - 3600)>


no ip ospf retransmit-interval
```

Defaults

5

Related commands

ip ospf dead-interval

ip ospf hello-interval

ip ospf transmit-delay

show ip ospf retransmission-list

ip ospf transmit-delay

Use this command to configure the estimated time it takes to transmit a link state update packet on the interface. Precede this command with no to set the default estimated time it takes to transmit a link state update packet on the interface.

Command mode

Interface configuration

Syntax

```
ip ospf transmit-delay <seconds (0 - 3600)>


no ip ospf transmit-delay
```

Defaults

1

Related commands

ip ospf dead-interval

ip ospf hello-interval

ip ospf retransmit-interval

neighbor

Use this command to specify a neighbor router and its priority. Precede this command with no to remove the neighbor or set the default value for the neighbor priority.

Command mode

Router configuration

Syntax

```
neighbor <neighbor-id> [priority  <priority value (0-255)>]


no neighbor <neighbor-id> [priority]
```

Variable definitions

This table describes the variables used in the neighbor command.

Variable	Value
neighbor-id	Specifies the neighbor router ID.
priority	Indicates a number value that specifies the router priority

Defaults

priority	1

Related commands

ip ospf network

ip ospf priority

show ip ospf neighbor

network

Use this command to define the interfaces on which OSPF runs and the area ID for those interfaces. Precede this command with no to disable OSPF routing for interfaces defined and to remove the area ID of that interface.

Command mode

Router configuration

Syntax

```
network <Network number> area <area-id> [unnum Vlan <PortNumber>]


no network <Network number> area <area-id> [unnum Vlan <PortNumber>]
```

Variable definitions

This table describes the variables used in the network command.

Variable	Value
Network number	Specifies the network type.
area	Specifies the area associated with the OSPF address range. It is specified as an IP address.
unnum Vlan	VLAN ID for which no ip address is configured.

Related commands

router ospf

show ip ospf—database

show ip ospf interface

passive-interface default

Use this command to suppress routing updates on all interfaces. Precede this command with no to enable routing updates on all interfaces.

Command mode

Router configuration

Syntax

```
passive-interface default


no passive-interface default
```

Related commands

passive-interface vlan

show ip ospf interface

show ip ospf request-list

passive-interface vlan

Use this command to suppress routing updates on an interface. Precede this command with no to enable routing updates on an interface.

Command mode

Router configuration

Syntax

```
passive-interface vlan <vlan-id(1-4094)>}

no passive-interface vlan <vlan-id(1-4094)>
```

Variable definitions

This table describes the variables used in the `passive-interface vlan` command.

Variable	Value
vlan-id	Specifies the LSA retransmissions for adjacencies belonging to the VLAN interface

Related commands

`passive-interface default`

`show ip ospf interface`

`show ip ospf request-list`

redistribute

Use this command to configure the protocol from which the routes have to be redistributed into OSPF . Precede this command with no to disable redistribution of routes from the given protocol into OSPF.

Command mode

Router configuration

Syntax

```
redistribute {static | connected | rip | bgp}


no redistribute {static | connected | rip | bgp}
```

Variable definitions

This table describes the variables used in the `redistribute` command.

Variable	Value
bgp	Advertises routes, that are learnt by the BGP process, in the OSPF routing process.
connected	Advertises directly connected networks routes, in the OSPF routing process.
rip	Advertises routes, that are learnt by the RIP process, in the OSPF routing process.
static	Advertises routes, configured statically, in the OSPF routing process.

Related commands

`default-information originate always`

`redist-config`

redist-config

Use this command to configure the information to be applied to routes learned from RTM. Precede this command with no to delete the information applied to routes learned from RTM.

Command mode

Router configuration

Syntax

```
redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>]
[metric-type {asExttype1 | asExttype2}]  [tag <tag-value>}


no redist-config <Network> <Mask>
```

Variable definitions

This table describes the variables used in the `redist-config` command.

Variable	Value
Mask	Specifies the mask of the destination route.
metric-type	Specifies the metric type applied to the route before it is advertised into the OSPF domain.
metric-value	Specifies the metric value applied to the route before it is advertised into the OSPF domain.
Network	Specifies the IP Address of the destination route.
tag	Specifies the tag type describes whether tags will be automatically generated or will be manually configured.

Defaults

metric-value	10
metric-type	asExttype2
tag	manual

Related commands

redistribute

router-id

Use this command to set the router-id for the OSPF process.

Command mode

Router configuration

Syntax

```
router-id <router ip address>
```

Variable definitions

This table describes the variables used in the `router-id` command.

Variable	Value
router ip address	Specifies the OSPF router ID as an IP address.

Related commands

`router ospf`

`show ip ospf route`

router ospf

Use this command to enable the OSPF routing process. Precede this command with no to disable the OSPF routing process.

Command mode

Global configuration

Syntax

```
router ospf


no router ospf
```

Related commands

network

router-id

show ip ospf—database

show ip ospf route

set nssa asbr-default-route translator

Use this command to enable or disable setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.

Command mode

Router configuration

Syntax

```
set nssa asbr-default-route translator {enable | disable}
```

Variable definitions

This table describes the variables used in the `set nssa asbr-default-route translator` command.

Variable	Value
enable	When set to enabled, P-Bit is set in the generated Type-7 default LSA.
disable	When set disabled, P-Bit is clear in the generated default LSA.

Defaults

Disabled

Related commands

ASBR Router

show ip ospf

Use this command to display general information about the OSPF routing process.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf
```

Related commands

area—stability-interval

area—virtual-link

debug ip ospf

ip ospf authentication-key

show ip ospf border-routers

Use this command to display OSPF border and boundary router information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf border-routers
```

Related commands

abr-type

ASBR Router

show ip ospf—database

Use this command to display OSPF database summary for the LSA type.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf [area-id] database {asbr-summary | external | network |
nssa-external | opaque-area | opaque-as | opaque-link | router | summary
} [link-state-id] [{adv-router <ip-address> | self-originate}]
```

Variable definitions

This table describes the variables used in the `show ip ospf-database` command.

Variable	Value
area-id	Specifies the area associated with the OSPF address range. It is specified as an IP address.
database	Displays how many of each type of LSA for each area there are in the database.
asbr-summary	Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.
external	Displays information only about the external LSAs.
network	Displays information only about the network LSAs.
nssa-external	Displays information only about the NSSA external LSAs.
opaque-area	Displays information about the Type-10 LSAs.
opaque-as	Displays information about the Type-11 LSAs.
opaque-link	Displays information about the Type-9 LSAs.
router	Displays information about the router LSAs.
summary	Displays information about the summary LSAs.
link-state-id	Portion of the internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address.
adv-router	Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself.
self-originate	Displays only self-originated LSAs (from the local router).

Related commands

`network`

`router ospf`

show ip ospf—database summary

Use this command to display OSPF LSA database summary.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf [area-id] database [{database-summary | self-originate |
adv-router <ip-address>}]
```

Variable definitions

This table describes the variables used in the `show ip ospf—database summary` command.

Variable	Value
area-id	Specifies area associated with the OSPF address range. It is specified as an IP address.
database	Displays how many of each type of LSA for each area there are in the database.
database-summary	Displays how many of each type of LSA for each area there are in the database, and the total number of LSA types.
self-originate	Displays only self-originated LSAs (from the local router).
adv-router	Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself.

Related commands

`summary-address`

show ip ospf interface

Use this command to display OSPF interface information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf interface {[vlan
<vlan-id(1-4094)]>|[<Interface-Type><Interface-Index>]}
```

Variable definitions

This table describes the variables used in the `show ip ospf interface` command.

Variable	Value
vlan	Specifies LSA retransmissions for adjacencies belonging to the VLAN interface.
Interface-Type	Specifies the type of interface.
Interface-Index	Specifies the interface index.

Related commands

`ip ospf cost`

`ip ospf dead-interval`

`ip ospf demand-circuit`

`ip ospf hello-interval`

`passive-interface default`

`passive-interface vlan`

show ip ospf neighbor

Use this command to display OSPF neighbor information list.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf neighbor {[vlan <vlan-id
(1-4094)>]|[<Interface-Type><Interface-Index>]} [Neighbor ID] [detail]
```

Variable definitions

This table describes variables used in the `show ip ospf neighbor` command.

Variable	Value
detail	Indicates OSPF neighbor information in detail.
Neighbor ID	Indicates neighbor router ID.
vlan	Specifies LSA retransmissions for adjacencies belonging to the VLAN interface.
Interface-Type	Specifies the type of the interface.
Interface-Index	Specifies the interface index.

Related commands

`neighbor`

show ip ospf request-list

Use this command to display link state request list information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf request-list [<neighbor-id>] {[vlan <vlan-id
(1-4094)>]|[<Interface-Type><Interface-Index>]}
```

Variable definitions

This table describes the variables used in the `show ip ospf request-list` command.

Variable	Value
neighbor-id	Specifies neighbor router ID.
vlan	Specifies LSA retransmissions for adjacencies belonging to the VLAN interface.

Related commands

`passive-interface default`

`passive-interface vlan`

show ip ospf retransmission-list

Use this command to display OSPF link state retransmission list information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf retransmission-list [<neighbor-id>]  {[vlan <vlan-id
(1-4094)>]|[<Interface-Type><Interface-Index>]}
```

Variable definitions

The table describes the variables used in the `show ip ospf retransmission-list` command.

Variable	Value
neighbor-id	Specifies neighbor router ID.
vlan	Specifies LSA retransmissions for adjacencies belonging to the VLAN interface.
Interfac-Type	Specifies the type of the interface.
Interface-Index	Specifies the interface index.

Related commands

`ip ospf retransmit-interval`

show ip ospf route

Use this command to display routes learned by OSPF process.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf route
```

Related commands

router-id

router ospf

show ip ospf—summary address

Use this command to display OSPF summary-address redistribution information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf {area-range | summary-address}
```

Variable definitions

The table describes the variables used in the `show ip ospf—summary address` command.

Variable	Value
area-range	Specifies area associated with the OSPF address range. It is specified as an IP address.
summary-address	Specifies aggregate addresses for OSPF.

Related commands

`area—range`

`summary-address`

show ip ospf virtual-links

Use this command to display OSPF virtual link information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip ospf virtual-links
```

Related commands

area—virtual-link

summary-address

Use this command to create aggregate addresses for OSPF. Precede this command with no to delete the external summary address.

Command mode

Router configuration

Syntax

```
summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll |
advertise | not-advertise}] [Translation {enabled | disabled}]


no summary-address <Network> <Mask> <AreaId>
```

Variable definitions

This table describes the variables used in the `summary-address` command.

Variable	Value
advertise	When set to advertise and associated areaId is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areaId is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x.
allowAll	When set to allowAll and associated areaId is 0.0.0.0 aggregated Type-5 are generated for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified range.
AreaId	Specifies area associated with the OSPF address range. It is specified as an IP address.
denyAll	When set to denyAll neither Type-5 nor Type-7 will be generated for the specified range.
Mask	Specifies the subnet mask that pertains to the range.
Network	Specifies the IP address of the net indicated by the range.
not-advertise	When set to doNotAdvertise (2) and associated areaId is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if associated areaId is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range.
Translation	Indicates how an NSSA Border router is performing NSSA translation of Type-7 to into Type-5 LSAs. When set to enabled, P Bit is set in the generated Type-7 LSA. When set to disabled P Bit is cleared in the generated Type-7 LSA for the range

Defaults

summary-address	advertise
translation	disabled

Related commands

area—range

ip ospf authentication-key

ip ospf message-digest-key

show ip ospf—database summary

show ip ospf—summary address

Session Initiation Protocol commands

The Session Initiation Protocol (SIP) module will be deployed in CAS. SIP module is responsible for routing the calls between endpoints and for the NAT ALG translation. SIP module hosts features like extension dialing, short number dialing and routing the calls to gateways etc.

SIP commands navigation

- add dialplan (page 518)
- add sipserver MaximumSimWANCallsAllowed (page 519)
- add subscriber (page 520)
- bsg (page 521)
- CDR Mode (page 522)
- delete dialplan (page 523)
- delete sipserver MaximumSimWANCallsAllowed (page 524)
- delete subscriber (page 525)
- dialplan (page 526)
- domain (page 527)
- protocolheader (page 528)
- proxypolicy (page 529)
- registration (page 530)
- reload dialplan (page 531)
- set sipserver (page 532)
- set sipserver BackupModeGlobalDialPlanName (page 533)
- set sipserver—Brief / Detailed Traces (page 534)
- set sipserver CDRDirectoryPath (page 535)
- set sipserver CDRGeneration (page 536)
- set sipserver DNSLookupTimeOut (page 537)
- set sipserver domain name (page 538)
- set sipserver Dynamic Subscriber (page 539)
- set sipserver EnableSessionTimerRangeValidations (page 540)
- set sipserver ForkingPolicy (page 541)
- set sipserver –max/min/default timers (page 542)
- set sipserver –max/min/default timers (page 542)
- set sipserver - MaximumRegistrationPeriod (page 543)
- set sipserver MaximumSimWANCallsAllowed (page 544)
- set sipserver MinimumRegistrationPeriod (page 545)
- set sipserver NormalModeGlobalDialPlanName (page 546)
- set sipserver OrganizationHeader (page 547)
- set sipserver PolledServers (page 548)

- set sipserver ServerHeader (page 549)
- set sipserver SIP Message Dumps (page 550)
- set sipserver TFTPServerAddress (page 551)
- set sipserver - timer (page 552)
- show sipserver ActiveWANCallCount (page 554)
- show sipserver CDRDirectoryPath (page 555)
- show sipserver CDRGeneration (page 556)
- show sipserver dialplan (page 557)
- show sipserver DynamicSubscriber (page 558)
- show sipserver NormalModeGlobalDialPlanName (page 559)
- show sipserver OrganizationHeader (page 560)
- show sipserver - Port (page 561)
- show sipserver - Registration (page 562)
- show sipserver –scope bsg (page 563)
- show sipserver serverdomainname (page 564)
- show sipserver – Session Timer (page 565)
- show sipserver status (page 566)
- show sipserver subscriber details (page 567)
- show sipserver TFTPServerAddress (page 568)
- show sipserver - Timer (page 569)
- show sipserver - Traces (page 570)
- sip (page 571)
- sip – enable/disable (page 572)
- timer (page 573)
- trace sip (page 574)
- traces (page 575)
- transport (page 576)
- update subscriber (page 577)

add dialplan

Use this command to upload a new dialplan.

Command mode

SIP configuration

Syntax

```
add dialplan <dialplanname> <dest_file_path>
```

Variable definitions

This table describes the variables used in the `add dialplan` command.

Variable	Value
dialplanname	Specifies the dial plan name.
dest_file_path	Specifies the path to the destination file

Related commands

delete dialplan

show sipserver dialplan

add sipserver MaximumSimWANCallsAllowed

Use this command to configure the maximum simultaneous calls allowed on each WAN link.

Command mode

SIP BSG configuration

Syntax

```
add sipserver MaximumSimWANCallsAllowed { WAN1 | WAN2 | WAN3 }
<MaxCalls(1-500)>
```

Variable definitions

This table describes the variables used in the `add sipserver MaximumSimWANCallsAllowed` command.

Variable	Value
WAN1 | WAN2 | WAN3	Specifies the different maximum sim WAN calls allowed.
MaxCalls	Specifies the maximum call value.

Related commands

set sipserver EnableSessionTimerRangeValidations

delete sipserver MaximumSimWANCallsAllowed

add subscriber

Use this command to add subscriber details.

Command mode

SIP Configuration

Syntax

```
add subscriber <user-name> <domain-name> [alias <alias-name>]
[calling-line-identity <subscriber_identity>]
```

Variable definitions

This table describes the variables used in the `add subscriber` command.

Variable	Value
user-name	Specifies the user name.
domain-name	Specifies the domain name.
alias	Specifies the alias.
calling-line-identity	Specifies the calling line identifier.

Related commands

delete subscriber

update subscriber

show sipserver subscriber details

bsg

Use this command to enter the BSG configuration mode.

Command mode

SIP Configuration

Syntax

```
bsg
```

CDR Mode

Use this command to enter the CDR configuration mode.

Command mode

SIP Configuration

Syntax

```
cdr
```

delete dialplan

Use this command to delete a dialplan.

Command mode

SIP Configuration

Syntax

```
delete dialplan <dialplanname>
```

Variable definitions

This table describes the variables used in the `delete dialplan` command.

Variable	Value
Dialplanname	Specifies the dialplan name.

Related commands

add dialplan

show sipserver dialplan

delete sipserver MaximumSimWANCallsAllowed

Use this command to delete the configured value of maximum calls allowed on each WAN link.

Command mode

SIP BSG configuration

Syntax

```
delete sipserver MaximumSimWANCallsAllowed { WAN1 | WAN2 | WAN3 }
<MaxCalls(1-500)>
```

Variable definitions

This table describes the variables used in the `delete sipserver MaximumSimWANCallsAllowed` command.

Variable	Value
WAN1 | WAN2 | WAN3	Specifies the different maximum sim WAN calls allowed.
MaxCalls	Specifies the maximum call value.

Related commands

set sipserver MaximumSimWANCallsAllowed

add sipserver MaximumSimWANCallsAllowed

show sipserver subscriber details

delete subscriber

Use this command to delete the subscriber details.

Command mode

SIP configuration

Syntax

```
delete subscriber <user-name> <domain-name>
```

Variable definitions

This table describes the variables used in the `delete subscriber` command.

Variable	Value
user-name	Specifies the user name.
domain-name	Specifies the domain name.

Related commands

add subscriber

update subscriber

show sipserver subscriber details

dialplan

Use this command to enter the dialplan configuration mode.

Command mode

SIP configuration

Syntax

```
dialplan
```

domain

Use this command to enter the domain configuration mode.

Command mode

SIP configuration

Syntax

```
domain
```

protocolheader

Use this command to enter the protocolheader configuration mode.

Command mode

SIP configuration

Syntax

```
protocolheader
```

proxypolicy

Use this command to enter the proxypolicy configuration mode.

Command mode

SIP configuration

Syntax

```
proxypolicy
```

registration

Use this command to enter the registration configuration mode.

Command mode

SIP configuration

Syntax

```
registration
```

reload dialplan

Use this command to reload a dialplan from Data Base (DB).

Command mode

SIP configuration

Syntax

```
reload dialplan {all | <dialplanname>}
```

Variable definitions

This table describes the variables used in the `reload dialplan` command.

Variable	Value
All	Specifies all dialplan.
dialplanname	Specifies the dialplan name.

Related commands

add dialplan

delete dialplan

show sipserver dialplan

set sipserver

Use this command to configure the ports on which the SIP server accepts requests.

Command mode

SIP transport configuration

Syntax

```
set sipserver {SIPTCPPort | SIPUDPPort | TLSListenPorts} <1024-65535>
```

Variable definitions

This table describes the variables used in the `set sipserver` command.

Variable	Value
SIPTCPPort	Specifies the TCP port number on which the SIP server must listen for incoming request.
SIPUDPPort	Specifies the UDP port number on which the SIP server must listen for incoming request.
TLSListenPorts	Specifies the TLS port number on which the SIP server must listen for incoming request.
1024-65535	Specifies the valid port number range.

Related commands

show sipserver ActiveWANCallCount

set sipserver BackupModeGlobalDialPlanName

Use this command to configure the name of the global dialplan used in backup mode.

Command mode

SIP dialplan configuration

Syntax

```
set sipserver BackupModeGlobalDialPlanName <dialplanname>
```

Variable definitions

This table describes the variables used in the `set sipserver BackupModeGlobalDialPlanName` command.

Variable	Value
dialplanname	Specifies the name of global dialplan to be used in backup mode.

Defaults

None

Related commands

show sipserver dialplan

set sipserver—Brief / Detailed Traces

Use this command to configure whether all the SIP messages processed by the SIP server are traced in brief or detail.

Command mode

SIP trace configuration

Syntax

```
set sipserver { BriefTraces | DetailedTraces } {{[ALG-CAC] [Registrar]
[CallServer] [RoutingEngine] [CarrierMonitoring]} All | None}>
```

Variable definitions

This table describes the variables used in the `set sipserver Brief—Detailed Traces` command.

Variable	Value
BriefTraces	Specifies the brief trace messages.
DetailedTraces	Specifies the detailed trace messages.

Related commands

show sipserver - Traces

set sipserver CDRDirectoryPath

Use this command to configure the directory for storing old CDR in a remote host.

Command mode

SIP CDR configuration

Syntax

```
set sipserver CDRDirectoryPath <Path>
```

Variable definitions

This table describes the variables used in the `set sipserver CDRDirectoryPath` command.

Variable	Value
Path	Specifies the CDR Directory Path.

set sipserver CDRGeneration

Use this command to configures the property for the SIP server.

Command mode

SIP CDR configuration

Syntax

```
set sipserver CDRGeneration {TRUE | FALSE}
```

Variable definitions

This table describes the variables used in the `set sipserver CDRGeneration` command.

Variable	Value
TRUE	Sets CDRGeneration option as true.
FALSE	Sets CDRGeneration option as false.

set sipserver DNSLookupTimeOut

This command configures the DNSLookupTimeOut in milliseconds after which DNS lookups attempted by the proxy must timeout.

Command mode

SIP ProxyPolicy Configuration

Syntax

```
set sipserver DNSLookupTimeOut <integer(1-4294967295)>
```

Variable definitions

This table describes the variables used in the `set sipserver DNSLookupTimeOut` command.

Variable	Value
integer	Specifies the DNS lookup timeout value.

Defaults

20000 milliseconds

Related commands

show sipserver OrganizationHeader

set sipserver domain name

Use this command to configure the domain name of the SIP server.

Command mode

SIP domain name configuration

Syntax

```
set serverdomainname <domain name>
```

Variable definitions

This table describes the variables used in the `set sipserver domain name` command.

Variable	Value
domain name	Specifies the domain name of the SIP server.

set sipserver Dynamic Subscriber

Use this command to enable or disable the dynamic subscriber addition or deletion.

Command mode

SIP registration configuration

Syntax

```
set sipserver {AddDynamicSubscriber | DeleteDynamicSubscriber} {TRUE |
FALSE}
```

Variable definitions

This table describes the variables used in the `set sipserver Dynamic Subscriber` command.

Variable	Value
AddDynamicSubscriber	Specifies addition of dynamic subscriber.
DeleteDynamicSubscriber	Specifies deletion of dynamic subscriber.
TRUE	Enables the dynamic subscriber addition or deletion.
FALSE	Disables the dynamic subscriber addition or deletion.

set sipserver EnableSessionTimerRangeValidations

Use this command to configure the property EnableSessionTimerRangeValidations that performs the session timer handling by the proxy server. The SIP server only controls the session timer periods requested by endpoints, it does not start the timer and keep track of sessions. Actual control of the session depends on the support at the endpoints.

Command mode

SIP timer configuration

Syntax

```
set sipserver EnableSessionTimerRangeValidations {TRUE | FALSE}
```

Variable definitions

This table describes the variables used in the `set sipserver EnableSessionTimerRangeValidations` command.

Variable	Value
TRUE	Enables the session timer.
FALSE	Disables the session timer.

Default

FALSE

Related commands

show sipserver - Timer

set sipserver ForkingPolicy

Use this command to configure the mode of forking in the proxy server.

Command mode

SIP ProxyPolicy configuration

Syntax

```
set sipserver ForkingPolicy {first-only | sequential | parallel}
```

Variable definitions

This table describes the variables used in the `set sipserver ForkingPolicy` command.

Variable	Value
first-only	Specifies the first-only forking policy.
sequential	Specifies the sequential forking policy.
parallel	Specifies the parallel forking policy.

Defaults

Sequential

Related commands

show sipserver - Registration

set sipserver –max/min/default timers

This command configures the session timers supported by proxy.

Command mode

SIP Timer Configuration

Syntax

```
set sipserver {MaximumSessionTimer |MinimumSessionTimer |
DefaultSessionTimer} <integer(90-4294967295)>
```

Variable definitions

This table describes the variables used in the `set sipserver –max/min/default timers` command.

Variable	Value
MaximumSessionTimer	Specifies the maximum session timer supported by proxy.
MinimumSessionTimer	Specifies the minimum session timer supported by proxy.
DefaultSessionTimer	Specifies the default session timer supported by proxy.

Defaults

MaximumSessionTime	3600 seconds
MinimumSessionTimer	90 seconds
DefaultSessionTimer	1800 seconds

Related commands

show sipserver – Session Timer

set sipserver - MaximumRegistrationPeriod

Use this command to configure properties of the SIP server like MaximumRegistrationPeriod, DefaultRegistrationPeriod, and MaxContacts per AoR.

Command mode

SIP registration configuration

Syntax

```
set sipserver {MaximumRegistrationPeriod | DefaultRegistrationPeriod |
MaxContactsPerAOR}<integer(1-4294967295)>
```

Variable definitions

This table describes the variables used in the `set sipserver - MaximumRegistrationPeriod` command.

Variable	Value
MaximumRegistrationPeriod	Specifies the maximum registration period for any phone when the BSG is in the backup mode. When a phone registers with an expires value greater than this parameter, will register with the same value as its expires parameter. Keep this value small (30 seconds) so that when the central SIP server becomes active and the BSG switches to the normal mode, the phones will re-register with the central SIP server within this timeframe.
DefaultRegistrationPeriod	Specifies the default registration period.
MaxContactsPerAOR	Specifies the maximum contacts per AOR.
integer	Specifies the registration value corresponding to either of the 3 registrations.

Defaults

MaximumRegistrationPeriod	3600
DefaultRegistrationPeriod	3600
MaxContactsPerAOR	5

Related commands

show sipserver - Registration

set sipserver MaximumSimWANCallsAllowed

Use this command to configure the maximum simultaneous calls allowed on each WAN link.

Command mode

SIP BSG configuration

Syntax

```
set sipserver MaximumSimWANCallsAllowed {[<WAN1 link> <MaxCalls(1-100)>]
[<WAN2 link> <MaxCalls(1-100)>] [<WAN3 link> <MaxCalls(1-100)>]}
```

Variable definitions

This table describes the variables used in the `set sipserver MaximumSimWANCallsAllowed` command.

Variable	Value
[<WAN1 link> <MaxCalls(1-500)>]	Specifies Different Maximum Sim WAN Calls Allowed for WAN1 link.
[<WAN2 link> <MaxCalls(1-500)>]	Specifies Different Maximum Sim WAN Calls Allowed for WAN2 link.
[<WAN3 link><MaxCalls(1-500)>]	Specifies Different Maximum Sim WAN Calls Allowed for WAN3 link.

Related commands

`add sipserver MaximumSimWANCallsAllowed`

`delete sipserver MaximumSimWANCallsAllowed`

set sipserver MinimumRegistrationPeriod

Use this command to configure the minimum registration period (MRP) of SIP server.

Command mode

SIP registration configuration

Syntax

```
set sipserver MinimumRegistrationPeriod <integer(1-3600)>
```

Variable definitions

This table describes the variables used in the `set sipserver MinimumRegistrationPeriod` command.

Variable	Value
integer	Specifies the value of MRP. SIP server returns a reject response message “423 Interval Too Brief In Expires Header” when a phone registers with an “expires” value less than this parameter.

Defaults

60

Related commands

`show sipserver - Registration`

set sipserver NormalModeGlobalDialPlanName

This command configures the name of the global dialplan.

Command mode

SIP Dialplan configuration

Syntax

```
set sipserver NormalModeGlobalDialPlanName <dialplanname>
```

Variable definitions

This table describes the variables used in the `set sipserver NormalModeGlobalDialPlanName` command.

Variable	Value
dialplanname	Specifies Normal Mode Global Dial Plan Name

Related commands

`show sipserver dialplan`

set sipserver OrganizationHeader

This command configures the organization name. Insert this name as organization header into the messages generated by the SIP server.

Command mode

SIP ProtocolHeader configuration

Syntax

```
set sipserver OrganizationHeader { [ipaddress <ipaddress>] | [hostname <hostname>]}
```

Variable definitions

This table describes the variables used in the `set sipserver OrganizationHeader` command.

Variable	Value
ipaddress	Specifies IPv4 Address.
hostname	Specifies host name.

Related commands

`show sipserver OrganizationHeader`

set sipserver PolledServers

This command configures the carrier network or SIP servers to be polled.

Command mode

SIP Domain configuration

Syntax

```
set  sipserver PolledServers Pollingaddress { ipaddress | hostname
<hostname>} {[port <1-65535>] [pollinterval <(10-600)seconds>]
[pollretries <1-10>] [transport { tcp | udp | tls}]}
```

Variable definitions

This table describes the variables used in the `set sipserver PolledServers Pollingaddress` command.

Variable	Value
ipaddress | hostname	Specifies the polling address.
port	Specifies the port number.
pollinterval	Specifies the poll interval.
pollretries	Specifies the poll retries.
transport	Specifies the transport type. The type can be either tcp or udp or tls.

Defaults

port	5060
pollinterval	30
pollretries	2
transport	udp

set sipserver ServerHeader

Use this command to specify the string to be used in the server header in responses generated by the SIP server.

Command mode

SIP ProtocolHeader configuration

Syntax

```
set sipserver ServerHeader <string>
```

Variable definitions

This table describes the variables used in the `set sipserver ServerHeader` command.

Variable	Value
string	Specifies the SIP server header string value.

Related commands

`show sipserver OrganizationHeader`

set sipserver SIP Message Dumps

Use this command to configure whether all the SIP messages processed by the SIP server must be traced or not.

Command mode

SIP Traces configuration

Syntax

```
sipserver SIPMessageDumps {TRUE | FALSE}
```

Variable definitions

This table describes the variables used in the `sipserver SIPMessageDumps` command.

Variable	Value
TRUE	Enables the traces for calls.
FALSE	Disables the traces for calls.

Defaults

FALSE

Related commands

`show sipserver - Traces`

set sipserver TFTPServerAddress

Use this command to configures the host where TFTP server is running to store old CDR files.

Command mode

SIP CDR configuration

Syntax

```
set sipserver TFTPServerAddress <IpAddress>
```

Variable definitions

This table describes the variables used in the `set sipserver TFTPServerAddress` command.

Variable	Value
IpAddress	Specifies the TFTP server IP Address.

set sipserver - timer

Use this command to configures different timers of the SIP server.

Command mode

SIP timer configuration

Syntax

```
set sipserver {{TimerT1 | TimerT2 | TimerB | TimerF | TimerH | TimerI |
TimerJ | TimerK} <integer(1-2147483647)> | {TimerC
<integer(180000-2147483647)>} | {TimerD <integer(32000-2147483647)>}}
```

Variable definitions

This table describes the variables used in the `set sipserver - timer` command.

Variable	Value
TimerT1 | TimerT2 | TimerB | TimerC | TimerF | TimerH | TimerI | TimerJ | TimerK	Specifies different timers. TimerT1 and TimerT2 are used for local retransmissions.
TimerD	Specifies the minimum value configurable for TimerD, which is 32000. The range is 32000 - 2147483647.
integer	Specifies timer value in milliseconds.

Defaults

TimerT1	500 ms
TimerT2	4000 ms
TimerB	64 *T1
TimerC	180 seconds
TimerD	32 seconds
TimerF	32 seconds
TimerH	32 seconds
TimerI	5 seconds
TimerJ	32 seconds
TimerK	5 seconds

Related commands

show sipserver subscriber details

show sipserver ActiveWANCallCount

Use this command to display the total active WAN call count.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver ActiveWANCallCount
```

show sipserver CDRDirectoryPath

Use this command to display the configuration properties of CDR directory path.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver CDRDirectoryPath
```

show sipserver CDRGeneration

Use this command to display the configuration properties of CDR generation.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver CDRGeneration
```

show sipserver dialplan

Use this command to display the dialplan configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver dialplan <dialplanname> <dest_file_path>
```

Variable definitions

This table describes the variables used in the `show sipserver dialplan` command.

Variable	Value
dialplanname	Displays dialplan name.
dest-file_path	Displays path of the destination file.

Related commands

`delete dialplan`

`add dialplan`

`reload dialplan`

show sipserver DynamicSubscriber

Use this command to display the configuration properties of the dynamic subscriber.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {AddDynamicSubscriber | DeleteDynamicSubscriber}
```

Variable definitions

This table describes the variables used in the `show sipserver DynamicSubscriber` command.

Variable	Value
AddDynamicSubscriber	Specifies the addition of the dynamic subscriber.
DeleteDynamicSubscriber	Specifies the deletion of the dynamic subscriber.

show sipserver NormalModeGlobalDialPlanName

Use this command to display the name of the global dialplan.

Command mode

Privileged EXEC or User EXEC

Syntax

show sipserver NormalModeGlobalDialPlanName

Related commands

`set sipserver NormalModeGlobalDialPlanName`

show sipserver OrganizationHeader

Use this command to display the configuration properties for scope server information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {PrivateSIPViaHost | OrganizationHeader |
PrivateSIPRecordRoute | PrivateSIPSRecordRoute | DNSLookupTimeOut |
ServerHeader }
```

Variable definitions

This table describes the variables used in the `show sipserver OrganizationHeader` command.

Variable	Value
PrivateSIPViaHost	Displays private SIP through host.
OrganizationHeader	Displays organization header.
PrivateSIPRecordRoute	Displays private SIP record route.
PrivateSIPSRecordRoute	Displays private SIP record route.
DNSLookupTimeOut	Displays DNS lookup timeout.
ServerHeade	Displays server header.

Related commands

`set sipserver OrganizationHeader`

`set sipserver ServerHeader`

`set sipserver DNSLookupTimeOut`

show sipserver - Port

Use this command to display ports on which SIP server accepts requests.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver { SIPTCPPort | SIPUDPPort | TLSListenPorts }
```

Variable definitions

This table describes the variables used in the `show sipserver - Port` command.

Variable	Value
SIPTCPPort	Specifies SIP TCP port.
SIPUDPPort	Specifies SIP UDP port.
TLSListenPorts	Specifies TLS listen ports.

Related commands

`set sipserver`

show sipserver - Registration

Use this command to display the configuration properties for scope registrar.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {MinimumRegistrationPeriod | MaximumRegistrationPeriod |
DefaultRegistrationPeriod | MaxContactsPerAOR }
```

Variable definitions

This table describes the variables used in the `show sipserver - Registration` command.

Variable	Value
MinimumRegistrationPeriod	Specifies minimum registration period.
MaximumRegistrationPeriod	Specifies maximum registration period.
DefaultRegistrationPeriod	Specifies default registration period.
MaxContactsPerAOR	Specifies maximum contacts per AOR.

Related commands

`set sipserver MinimumRegistrationPeriod`

`set sipserver MaximumSimWANCallsAllowed`

show sipserver –scope bsg

Use this command to display the configuration properties for scope BSG.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {BackupModeGlobalDialPlanName | PolledServers |
MaximumSimWanCallsAllowed | IdleTimerForNATBindingRemoval |
PublicSIPViaHost | PublicSIPRecordRoute | PublicSIPSRecordRoute |
HostNameForWanLinks }
```

Variable definitions

This table describes the variables used in the `show sipserver –scope bsg` command.

Variable	Value
BackupModeGlobalDialPlanName	Displays backup mode global dialplan name.
PolledServers	Displays polled servers.
MaximumSimWanCallsAllowed	Displays maximum Sim WAN Calls Allowed (SWCA).
IdleTimerForNATBindingRemoval	Displays idle timer for NAT binding removal entry.
PublicSIPViaHost	Displays SIP host address for public via header.
PublicSIPRecordRoute	Displays SIP record route header used in public domain.
PublicSIPSRecordRoute	Displays SIP record route header used in public domain.
HostNameForWanLinks	Displays host name for WAN links.

Related commands

`set sipserver –max/min/default timers`

`set sipserver PolledServers`

`set sipserver MaximumSimWANCallsAllowed`

`add sipserver MaximumSimWANCallsAllowed`

`delete sipserver MaximumSimWANCallsAllowed`

show sipserver serverdomainname

Use this command to display the domain name of the SIP server.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver serverdomainname
```

show sipserver – Session Timer

Use this command to display the configuration properties for scope TransactionStatefulProxy.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver { EnableSessionTimerRangeValidations | ForkingPolicy |
MaximumSessionTimer | MinimumSessionTimer | DefaultSessionTimer }
```

Variable definitions

This table describes the variables used in the `show sipserver – Session Timer` command.

Variable	Value
EnableSessionTimerRangeValidations	Enables Session Timer Range Validations.
ForkingPolicy	Displays Forking Policy.
MaximumSessionTimer	Displays Maximum Session Timer (MST).
MinimumSessionTimer	Displays Minimum Session Timer (MST).
DefaultsessionTimer	Displays Default Session Timer (DST).

Related commands

`set sipserver –max/min/default timers`

`set sipserver`

set sipserver MaximumSimWANCallsAllowed

show sipserver status

Use this command to display the status of the CCLI server or the SIP server.

Command mode

Privileged EXEC or User EXEC

Syntax

show sipserver status

show sipserver subscriber details

Use this command to display the subscriber details.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver subscriber details  {all | {<user-name> <domain-name>}}
```

Variable definitions

This table describes the variables used in the `show sipserver subscriber details` command.

Variable	Value
all	Displays all the details.
<user-name> <domain-name>	Displays user specific details.

Related commands

`add subscriber`

`delete subscriber`

`update subscriber`

show sipserver TFTPServerAddress

Use this command to display the configuration properties of the TFTP server.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver TFTPServerAddress
```

show sipserver - Timer

Use this command to display the configuration properties for scope stack component.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {TimerT1 | TimerT2 | TimerB | TimerC | TimerD | TimerF |
TimerH | TimerI | TimerJ | TimerK }
```

Variable definitions

This table describes the variables used in the `show sipserver - Timer` command.

Variable	Value
TimerT1 | TimerT2 | TimerB | TimerC | TimerD | TimerF | TimerH | TimerI | TimerJ | TimerK	Displays different types of timers.

Related commands

`show sipserver subscriber details`

show sipserver - Traces

Use this command to display the configuration properties for scope diagnostics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sipserver {SIPMessageDumps | DetailedTraces | BriefTraces}
```

Variable definitions

This table describes the variables used in the `show sipserver - Traces` command.

Variable	Value
SIPMessageDumps	SIP Message Dumps
DetailedTraces	Detailed Traces
BriefTraces	Brief Traces

Related commands

`set sipserver SIP Message Dumps`

sip

This command enters the SIP configuration mode.

Command mode

Global configuration

Syntax

```
sip
```

sip – enable/disable

Use this command to enable or to disable the SIP server.

Command mode

SIP configuration

Syntax

```
sip {enable |disable}
```

Variable definitions

This table describes the variables used in the `sip – enable/disable` command.

Variable	Value
enable	Enables the SIP server.
disable	Disables the SIP server.

timer

Use this command to enter the timer configuration mode.

Command mode

SIP configuration

Syntax

```
timer
```

trace sip

Use this command to configure the SIP trace.

Command mode

Privileged EXEC or User EXEC

Syntax

```
trace sip {on|off}
```

Variable definitions

This table describes the variables used in the `trace sip` command.

Variable	Value
On|off	Specifies the SIP trace mode which can be ON or OFF.

traces

Use this command to enter the trace error configuration mode.

Command mode

SIP configuration

Syntax

```
traces
```

transport

Use this command to enter the transport configuration mode.

Command mode

SIP Configuration

Syntax

```
transport
```

update subscriber

Use this command to modify the subscriber details.

Command mode

SIP Configuration

Syntax

```
update subscriber <user-name> <domain-name> [alias <aliasname>]
[calling-line-identity <subsidentity>]
```

Variable definitions

This table describes the variables used in the `update subscriber` command.

Variable	Value
user-name-	Specifies the user name.
domain-name	Specifies the domain name.
alias	Specifies the alias name.
calling-line-identity	Specifies the Calling Line Identifier (CLI).

Related commands

`add subscriber`

`delete subscriber`

`show sipserver subscriber details`

Linux tunnel commands

The linux tunnel module creates a tunnel interface in the linux kernel. Use the linux kernel for injecting IP frames from user space program to linux IP stack available in kernel space. This tunnel interface can be used for communicating to native linux application or any other application running over linux IP stack.

One of the BSG system IP (vlan1) address is assigned to this tunnel. For the outside world, tunnel interface is not visible and is purely behind BSG system.

Linux tunnel commands navigation

- clear dns—server cache (page 579)
- copy (page 580)
- copy ftp (page 581)
- dns-server forwarder (page 583)
- dns-server forwarder – enable/disable (page 584)
- dns-server forwarder zone (page 585)
- set dns—server cache timeout (page 586)
- show dns (page 587)
- show tftp (page 588)
- telnet (page 589)
- tftp-server (page 590)
- tftp-server topdir (page 591)

clear dns—server cache

Use this command to clear the cached entries created by the earlier DNS queries.

Command mode

Global configuration

Syntax

```
clear dns-server cache
```

Related commands

show dns

copy

Use this command to send a file to the remote location.

Command mode

Privileged EXEC or User EXEC

Syntax

```
copy {  <LocalFile>  ftp <user-name> <password> <ip_addr> <RemoteFile>
```

Variable definitions

This table describes the variables used in the `copy` command.

Variable	Value
user-name	Specifies the user name to access the remote location.
password	Specifies the password.
ip_addr	Specifies the IP address.
RemoteFile	Specifies the remote file path.

Related commands

copy ftp

Use this command to receive a file from the remote location.

Command mode

Privileged EXEC or User EXEC

Syntax

```
copy ftp <user-name> <password> <ip_addr> <RemoteFile> <LocalFile>
```

Variable definitions

This table describes the variables used in the `copy ftp` command.

Variable	Value
user-name	Specifies the user name to access the remote location.
password	Specifies the password.
ip_addr	Specifies the IP address.
RemoteFile	Specifies the remote file path.
LocalFile	Specifies the path of the local file.

Related commands

debug linuxtun

Use this command to enable the trace messages for linuxtun-related applications. Precede this command with `no` to disable the trace messages.

Command mode

Privileged EXEC

Syntax

```
debug linuxtun { all | tftp | ftp | dns | telnet | secure }

no debug linuxtun { all | tftp | ftp | dns | telnet | secure }
```

Variable definitions

This table describes the variables used in the `debug linuxtun` command.

Variable	Value
all	Specifies all linux tunnel traces.
tftp	Specifies TFTP-related traces.
ftp	Specifies FTP-related traces.
dns	Specifies DNS-related traces.
telnet	Specifies Telnet-related traces.
secure	Specifies security-related traces.

dns-server forwarder

Use this command to set primary or secondary or both IP addresses for dns-forwarder. Precede this command with `no` to remove primary or secondary IP addresses for dns-forwarder.

Command mode

Global configuration

Syntax

```
dns-server forwarder [primary <unicast_ip_addr>] [secondary <
unicast_ip_addr>]


no dns-server forwarder {primary <unicast_ip_addr> | secondary <
unicast_ip_addr>}
```

Variable definitions

This table describes the variables used in the `dns-server forwarder` command.

Variable	Value
primary	Specifies primary IP address for dns-forwarder.
secondary	Specifies the secondary IP address for dns-forwarder.
unicast_ip_addr	Specifies the unicast IP address.

Related commands

show dns

dns-server forwarder – enable/disable

Use this command to enable or disable the dns-forwarder functionality.

Command mode

Global configuration

Syntax

```
dns-server forwarder { enable | disable }
```

Variable definitions

This table describes the variables used in the `dns-server forwarder – enable/disable` command.

Variable	Value
enable	Enables dns-forwarder functionality.
disable	Disables dns-forwarder functionality.

Defaults

Disable

Related commands

show dns

dns-server forwarder zone

Use this command to add a zone and add or remove the host entries. Precede the command with `no` to remove a zone and its all host entries.

Command mode

Global configuration

Syntax

```
dns-server forwarder zone < zone_name > {addRR <host_name>
<host_unicast_ip_addr> | removeRR <<host_name> <host_unicast_ip_addr> }


no dns-server forwarder zone < zone_name >
```

Variable definitions

This table describes the variables used in the `dns-server forwarder zone` command.

Variable	Value
zone_name	Adds a zone name.
addRR	Adds host entries.
removeRR	Removes host entries.
host_name	Adds a host name.
host_unicast_ip_addr	Specifies unicast IP address of the host.

Related commands

show dns

set dns—server cache timeout

Use this command to set the dns cache time.

Command mode

Global configuration

Syntax

```
set dns—server cache timeout <seconds>
```

Related commands

show dns

show dns

Use this command to show domain name server (DNS) server and list local host entries.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dns [listRR]
```

Variable definitions

This table describes the variables used in the `show dns` command.

Variable	Value
listRR	Specifies the DNS server and list local host entries.

Related commands

dns-server forwarder – enable/disable

dns-server forwarder

dns-server forwarder zone

show tftp

Use this command to display the trivial file transfer protocol (TFTP) server IP address, current status and the top directory.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show tftp
```

Related commands

tftp-server

telnet

Use this command to open a telnet session to remote host.

Command mode

Privileged Exec

Syntax

```
telnet [-l user ] HostIp [Port]
```

Variable definitions

This table describes the variables used in the `telnet` command.

Variable	Value
-l user	Specifies the login name of the user
HostIp	Specifies the host IP address.
Port	Specifies the port number. Value ranges from 1to 65535.

Defaults

Port	23

tftp-server

This command enables the TFTP server. Precede this command with `no` to disable the TFTP server.

Command mode

Global Configuration

Syntax

```
tftp-server
```

```
no tftp-server
```

Related commands

tftp-server topdir

show tftp

tftp-server topdir

Use this command to change the tftp-server directory from where the TFTP clients read or write files.

Command mode

Global Configuration

Syntax

```
tftp-server topdir <dirname(128)>
```

Variable definitions

This table describes the variables used in the `tftp-server topdir` command.

Variable	Value
dirname	Specifies the directory name. Maximum length of directory name is 128.

Defaults

/tftpboot

Related commands

tftp-server

show tftp

BSG commands

This section describes the commands to configure the Business Service Gateway (BSG) Command Line Interface (CLI).

BSG commands navigation

- Point-to-Point Protocol commands (page 631)
- Simple Network Time Protocol commands (page 641)
- Network Address Translation commands (page 652)
- Virtual private network policy commands (page 672)
- Diffserv commands (page 697)
- Access control list commands (page 721)
- VOIP commands (page 729)
- Technical Report 069 commands (page 769)

Firewall commands

Firewall is a complete security solution. It enables small to medium-sized business enterprises to securely interconnect computers on the office network to the internet, and protects them from external attacks and intrusions.

An organization can define its fundamental security policy using one of the following firewall techniques:

- Block all packets that are not explicitly configured to allow into the protected network.
- Allow all packets that are not explicitly configured to block from the protected network.

When the firewall is configured and administered, it defends any network against external threats. Because the firewall protects the network from outside threats, the private network is prevented from any unauthorized access using filters and stateful inspection of packets.

Firewall commands navigation

- access-list (page 596)
- clear global statistics (page 597)
- clear interface statistics (page 598)
- commit (page 599)
- disable (page 600)
- dmz (page 601)
- enable (page 602)
- filter add (page 603)
- firewall (page 604)
- icmp (page 605)
- icmp inspect (page 606)
- ip filter fragments large (page 607)
- ip inspect option (page 608)
- ip inspect tcp enable (page 609)
- ip inspect tcp half open (page 610)
- ip inspect tcp syn wait (page 611)
- ip verify reverse path (page 612)
- netbios filtering (page 613)
- no filter (page 614)
- show firewall access-lists (page 615)
- show firewall config (page 616)
- show firewall dmz host (page 617)
- show firewall filters (page 618)
- show firewall half open connections (page 619)
- show firewall interface config (page 620)

- show firewall interface statistics (page 621)
- show firewall logs (page 622)
- show firewall stateful table (page 623)
- show firewall stats (page 624)
- show url filters (page 625)
- trap threshold (page 626)
- untrusted port (page 627)
- url filter add (page 628)
- url filter delete (page 629)
- url filtering (page 630)

access-list

Use this command to add an access list or rule for the WAN interface. Precede this command with no to delete an existing rule in the firewall access list table.

Command mode

Firewall configuration

Syntax

```
access-list <acl name> {in|out} <filter name> {permit|deny} <priority
val> [log {brief|detail|none}]  [fragment {permit|deny}]

no access-list <acl name> {in|out}
```

Variable definitions

This table describes the variables used in the `access-list` command.

Variable	Value
acl name	Specifies the Access Control List (ACL) name.
in|out	Specifies the direction of the packet, which can be inbound or outbound).
filter name	Enter the filter name.
permit|deny	Specifies the action of the rule.
priority val	Specifies the priority value for the ACL. The value ranges from 1 to 255.
log {brief|detail|none}	Specifies the level of the log.
fragment {permit|deny}	Specifies the state of the fragmented packets. The state can be permitted or denied.

Related commands

`show firewall access-lists`

clear global statistics

Use this command to clear the firewall global statistics.

Command mode

Firewall configuration

Syntax

```
clear global statistics
```

Related commands

show firewall interface config

clear interface statistics

Use this command to clear the firewall statistics for a given interface.

Command mode

Firewall configuration

Syntax

```
clear interface statistics ([<interface-type> <0/a-b, 0/c, ...>]
[<interface-type> <0/a-b, 0/c, ...>] [{ppp|multilink} <a,b,c-d>] [vlan
<a,b,c-d>])
```

Related commands

show firewall interface statistics

commit

Use this command to delete or modify stateful table entries if the rules are changed.

Command mode

Firewall configuration

Syntax

```
commit
```

disable

Use this command to disable the firewall service.

Command mode

Firewall configuration

Syntax

```
disable
```

Related commands

`show firewall config`

dmz

Use this command to set the Demilitarized Zone (DMZ) host in the Local LAN. Precede this command with no to remove the DMZ host access.

Command mode

Firewall configuration

Syntax

```
dmz <DMZ host IP>


no dmz <DMZ host IP>
```

Variable definitions

This table describes the variables used in the dmz command.

Variable	Value
DMZ host IP	Specifies the IP address of the DMZ host.

Related commands

show firewall dmz host

enable

Use this command to enable firewall service.

Command mode

Firewall configuration

Syntax

```
enable
```

Related commands

`show firewall config`

filter add

Use this command to add a firewall filter based on IP address range, protocol, and port.

Command mode

Firewall configuration

Syntax

```
filter add <filter name> {src ip/range|any} {dest ip/range|any}
[<tcp|udp|icmp|igmp|ggp|ip|egp|igp|nvp|rsvp|igrp|ospf|any|other
<1-255>>] [srcport <range>] [destport <range>]
```

Variable definitions

This table describes the variables used in the `filter add` command.

Variable	Value
filter name	Specifies the filter name.
src ip/range|any	Specifies the range of source IP address or all source IP address.
dest ip/range|any	Specifies the range of destination IP address or all source IP address.
tcp|udp|icmp|igmp|ggp| ip|egp|igp|nvp|rsvp| igrp|ospf|any	Specifies the protocol of the incoming packets.
srcport <range>	Specifies the range of source ports.
destport <range>	Specifies the range of destination ports.

Related commands

`show firewall filters`

firewall

Use this command to enter into the firewall configuration mode.

Command mode

Global configuration

Syntax

```
firewall
```

icmp

Use this command to generate or suppress Internet Control Message Protocol (ICMP) message when firewall rejects a packet.

Command mode

Firewall configuration

Syntax

```
icmp {generate | suppress}
```

Variable definitions

This table describes the variables used in the `icmp` command.

Variable	Value
generate	Generates the ICMP message when firewall rejects a packet.
suppress	Suppresses the ICMP message when firewall rejects a packet.

Defaults

Disabled

Related commands

`show firewall config`

icmp inspect

Use this command to discard ping requests arriving on the WAN interface. Precede this command with no to allow the ping requests arriving on WAN interface.

Command mode

Firewall configuration

Syntax

```
icmp inspect
```

```
no icmp inspect
```

Defaults

Disabled

Related commands

show firewall config

ip filter fragments large

Use this command to set the size of IP filter fragmentation. Precede this command with `no` to remove the IP filter fragmentation.

Command mode

Firewall configuration

Syntax

```
ip filter fragments large <frag size>


no ip filter fragments
```

Variable definitions

This table describes the variables used in the `ip filter fragments large` command.

Variable	Value
frag size	Specifies the fragment size. The value ranges from 1 to 65,500.

Defaults

frag size	30,000

Related commands

`show firewall config`

ip inspect option

Use this command to set IP inspect option for the WAN interface. Precede this command with no to remove IP options of the packet.

Command mode

Firewall configuration

Syntax

```
ip inspect option {srcroute | recordroute | timestamp | any | trcroute}

no ip inspect option
```

Variable definitions

This table describes the variables used in the `ip inspect option` command.

Variable	Value
srcroute	Specifies the source route IP option.
recordroute	Specifies the record route IP option.
timestamp	Specifies the timestamp IP option.
any	Specifies any type of IP option.
trcroute	Specifies the trace route IP option.

Defaults

Any

Related commands

`show firewall config`

ip inspect tcp enable

Use this command to enable examining the TCP SYN packets. Precede this command with no to disable TCP SYN packets examination.

Command mode

Firewall configuration

Syntax

```
ip inspect tcp enable
```

```
no ip inspect tcp
```

Defaults

Enabled

Related commands

show firewall config

ip inspect tcp half open

Use this command to set the number of TCP connection requests that enters firewall module.

Command mode

Firewall configuration

Syntax

```
ip inspect tcp half open <no of TCP SYN packets>
```

Variable definitions

This table describes the variables used in the `ip inspect tcp half open` command.

Variable	Value
no of TCP SYN packets	Specifies the number of TCP connection requests entering the firewall module.

Defaults

no of TCP SYN packets	50

Related commands

`show firewall config`

ip inspect tcp syn wait

Use this command to set TCP SYN timeout interval in seconds.

Command mode

Firewall configuration

Syntax

```
ip inspect tcp syn wait <seconds>
```

Variable definitions

This table describes the variables used in the `ip inspect tcp syn wait` command.

Variable	Value
seconds	TCP SYN timeout interval.

Defaults

1

Related commands

`show firewall config`

ip verify reverse path

Use this command to enable IP spoof filtering mechanism. Precede this command with no to disable IP spoof filtering mechanism.

Command mode

Firewall configuration

Syntax

```
ip verify reverse path
```

```
no ip verify reverse path
```

Defaults

Enabled

Related commands

show firewall config

netbios filtering

Use this command to enable or disable netbios filtering.

Command mode

Firewall configuration

Syntax

```
netbios filtering {enable | disable}
```

Variable definitions

This table describes the variables used in the `netbios filtering` command.

Variable	Value
enable	Enables netbios filtering.
disable	Disables netbios filtering.

Defaults

Disabled

Related commands

`show firewall config`

no filter

Use this command to delete a filter in the firewall.

Command mode

Firewall configuration

Syntax

```
no filter <filter>
```

Variable definitions

This table describes the variables used in the `no filter` command.

Variable	Value
filter	Specifies the filter name.

Related commands

`filter add`

`show firewall filters`

show firewall access-lists

Use this command to display the access lists configured in the firewall.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall access-lists
```

Related commands

access-list

show firewall config

Use this command to display the current firewall configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall config
```

Related commands

disable

ip filter fragments large

ip inspect option

ip inspect tcp half open

show firewall dmz host

Use this command to display the configured DMZ hosts.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall dmz host
```

Related commands

dmz

show firewall filters

Use this command to display the filters configured in the firewall.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall filters
```

Related commands

`filter add`

show firewall half open connections

Use this command to display the Transmission Control Protocol (TCP) half open entries of the firewall. When the TCP 3-way handshake is complete, the entries will be removed. To see the entries for TCP established connections, refer this command `show firewall stateful table`.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall half open connections
```

Related commands

`ip inspect tcp half open`

show firewall interface config

Use this command to display the firewall interface configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall interface config
```

Related commands

show firewall config

show firewall interface statistics

Use this command to display interface specific statistics of the packets processed by the firewall.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall interface statistics { [Fast/Gig/PPP Port] | [Vlan Id] |
all }
```

show firewall logs

Use this command to display the events logged by the firewall.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall logs
```

show firewall stateful table

Use this command to display the stateful table entries.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall stateful table
```

show firewall stats

Use this command to display statistics of the packets processed by the firewall.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show firewall stats
```

Related commands

access-list

filter add

icmp inspect

ip inspect option

ip inspect tcp half open

show url filters

Use this command to display the list of URL filters.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show url filters
```

Related commands

`show firewall config`

trap threshold

Use this command to configure the global threshold, the maximum packet discard count. The SNMP manager receives the trap if the count is more than the global threshold.

Command mode

Firewall configuration

Syntax

```
trap threshold <Max Packet Discard Count>
```

Variable definitions

This table describes the variables used in the `trap threshold` command.

Variable	Value
Max Packet Discard Count	Specifies the global threshold count.

Related commands

`show firewall config`

untrusted port

Use this command to configure the interface type as untrusted to apply firewall on this interface.

Command mode

Firewall configuration

Syntax

```
untrusted port ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type>
<0/a-b, 0/c, ...>] [{ppp|multilink} <a,b,c-d>] [vlan <a,b,c-d>])
[trap-threshold <Max Packet Discard Count>]


no untrusted port ([<interface-type> <0/a-b, 0/c, ...>]
[<interface-type> <0/a-b, 0/c, ...>] [{ppp|multilink} <a,b,c-d>] [vlan
<a,b,c-d>])
```

Variable definitions

This table describes the variables used in the `untrusted port` command.

Variable	Value
<interface-type> <0/a-b, 0/c, ...>	Specifies the type of port interface and port ID. The interface can be gigabit ethernet type or fastethernet type.
ppp|multilink <a,b,c-d>	Specifies the untrusted Point to Point Protocol (PPP) or multilink PPP links.
vlan <a,b,c-d>	Specifies the untrusted VLAN links.
trap-threshold <Max Packet Discard Count>]	Specifies the threshold above which trap is sent to the SNMP manager configured.

Related commands

`show firewall config`

url filter add

Use this command to add a URL filter to the existing list of URL filters in the firewall.

Command mode

Firewall configuration

Syntax

```
url filter add <URL-String>
```

Variable definitions

This table describes the variables used in the `url filter add` command.

Variable	Value
URL-String	Specifies the IP address or URL string. The maximum length of the URL string is 99.

Related commands

`show firewall config`

url filter delete

Use this command to delete an URL filter from the existing list of URL filters in the firewall.

Command mode

Firewall configuration

Syntax

```
url filter delete <URL-String>
```

Variable definitions

This table describes the variables used in the `url filter delete` command.

Variable	Value
URL-String	Specifies the IP address or URL string of the filter to be delete.

Related commands

`show firewall config`

url filtering

Use this command to enable or disable URL filtering for addition or deletion of URL filters.

Command mode

Firewall configuration

Syntax

```
url filtering {enable | disable}
```

Variable definitions

This table describes the variables used in the `url filtering` command.

Variable	Value
enable	Enables the URL filtering.
disable	Disables the URL filtering.

Defaults

Disabled

Related commands

`show firewall config`

Point-to-Point Protocol commands

The Point-to-Point Protocol (PPP) interface provides a point-to-point link between two communicating ends [for example, BSG and the other end of the wide area network (WAN) connection]. This interface also provides the front end for getting the statistics of the PPP connection. These commands are executed only on BSG 12 platform.

PPP commands navigation

- debug ppp (page 632)
- keep-alive timeout (page 633)
- layer (page 634)
- multilink-group (page 635)
- peer (page 636)
- ppp authenticate username (page 637)
- ppp chap hostname (page 638)
- ppp username (page 639)
- uplink rate limit (page 640)

debug ppp

Use this command to set the debug level for tracing PPP module.

Command mode

Privileged EXEC

Syntax

```
debug ppp { all | [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall]
[buffer] | none }
```

Variable definitions

This table describes the variables used in the `debug ppp` command.

Variable	Value
all	Specifies all traces.
initshut	Specifies the initialization and shutdown traces.
mgmt	Specifies the management traces
data	Specifies the data traces.
ctpl	Specifies the control plane traces.
dump	Specifies the dump messages.
os	Specifies the Operating System (OS) related traces.
failall	Specifies the failure traces.
buffer	Specifies the buffer related traces.
none	Specifies not to remove traces.

Defaults

Debugging

keep-alive timeout

Use this command to set the keep-alive timeout value for a PPP link. The keep-alive timeout value denotes that the connection will be lost if no Echo response packet is received within the timeout value. The no form of the command disables the keep-alive checks.

Command mode

PPP Interface Configuration

Syntax

```
keep-alive timeout <keep-alive timeout value (1-600)>


no keep-alive timeout
```

Variable definitions

This table describes the variables used in the `keep-alive timeout` command.

Variable	Value
keep-alive timeout value	Specifies the keep-alive timeout value for a PPP link in seconds.Value ranges from 0 to 600.

Defaults

10

layer

Use this command to attach a virtual PPP link to a physical ethernet, serial or PVC interface. Precede this command with `no` to detach a virtual PPP link from the physical interface to which it is attached.

Command mode

PPP Interface Configuration

Syntax

```
layer {serial <interface-index> | pvc <interface-index> |
<interface-name> <interface-id>}


no layer
```

Variable definitions

This table describes the variables used in the `layer` command.

Variable	Value
serial	Specifies the serial interface to attach to the virtual PPP link.
pvc	Specifies the PVC channel to attach to the virtual PPP link.
interface-name	Specifies the ethernet interface name to attach to the virtual PPP link.
interface-id	Specifies the interface identifier.

multilink-group

Use this command to enable the multilink capability on a PPP link and to add it to the specified multilink bundle. Precede this command with `no` to disable the multilink capability on a PPP link and to remove it from the multilink bundle to which it is added.

Command mode

PPP Interface Configuration

Syntax

```
multilink-group <multilink-bundle-number>


no multilink-group <multilink-bundle-number>
```

Variable definitions

This table describes the variables used in the `multilink-group` command.

Variable	Value
multilink-bundle-number	Specifies the bundle number. Multilink capability attaches to this bundle number.

Related commands

layer

peer

Use this command to configure the peer IP address or DNS name offers during negotiation. Precede this command with no to reset the peer IP address or DNS name offered during negotiation.

Command mode

PPP Interface configuration

Syntax

```
peer {[ip address <ip-address>] [dns-address <dns-ip-address>]}

no peer {[ip address <ip-address>] [dns-address <dns-ip-address>]}
```

Variable definitions

This table describes the variables used in the peer command.

Variable	Value
ip address	Specifies the peer IP address.
dns-address	Specifies the DNS address.

ppp authenticate username

Use this command to allow an authentication to a specified user at the called side. Precede the command with `no` to deny authentication for the specified user.

Command mode

PPP interface configuration or Multilink PPP interface configuration

Syntax

```
ppp authenticate username <user-name> password <password>


no ppp authenticate username
```

Variable definitions

This table describes the variables used in the `ppp authenticate username` command.

Variable	Value
user-name	Specifies the PPP user name to be authenticated.
password	Specifies the PPP Password to be authenticated.

ppp chap hostname

Use this command to set the hostname sent in the CHAP challenge packets.

Command mode

PPP interface configuration or Multilink PPP interface configuration

Syntax

```
ppp chap hostname <link-hostname>
```

Variable definitions

This table describes the variables used in the `ppp chap hostname` command.

Variable	Value
link-hostname	Specifies the hostname sent in the CHAP challenge packets for the specified link.

ppp username

Use this command to get login details (username and password) at the calling side. Precede the command with `no` to remove the login details at the calling side.

Command mode

PPP interface configuration or Multilink PPP interface configuration

Syntax

```
ppp username <user-name> password <password>


no ppp username
```

Variable definitions

This table describes the variables used in the `ppp username` command.

Variable	Value
user-name	Specifies the PPP user name to be sent for authentication.
password	Specifies the PPP password to be sent for authentication.

uplink rate limit

Use this command to configure the output channel rate.

Command mode

Global configuration

Syntax

```
uplink rate limit <speed((100000-100000000) in bps)>
```

Variable definitions

This table describes the variables used in the `uplink rate limit` command.

Variable	Value
speed	Specifies the uplink rate which is applied over a specified interface.

Simple Network Time Protocol commands

The Simple Network Time Protocol (SNTP) module synchronizes the time and date in BSG by contacting the SNTP server. SNTP supports different time zones.

SNTP commands navigation

- clock summer-time recurring (page 642)
- show sntp clock (page 643)
- show sntp status (page 644)
- sntp (page 645)
- sntp authentication-key (page 646)
- sntp—enable/disable (page 647)
- sntp no time zone (page 648)
- sntp server (page 649)
- sntp set poll-interval (page 650)
- sntp time zone (page 651)

clock summer-time recurring

Use this command to enable Daylight Saving Time (DST). Precede this command with `no` to disable the DST.

Command mode

SNTP Configuration

Syntax

```
clock summer-time recurring <Week> <Day> <Month> <Time in Hours> <Week>
<Day> <Month> <Time in Hours>


no clock summer-time
```

Variable definitions

This table describes the variables used in the `clock summer-time recurring` command.

Variable	Value
Week Day Month	Specifies the format as First Sun Mar.
Time in Hours	Enter the value as 20 minutes.

show sntp clock

Use this command to display the current time.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sntp clock
```

Related commands

`sntp no time zone`

`sntp time zone`

show sntp status

Use this command to display SNTP status (Running or Not Running), SNTP server's IP Address, SNTP authentication type, and GMT Time Difference (+/- Hours:Minutes).

Command mode

Privileged EXEC or User EXEC

Syntax

```
show sntp status
```

Related commands

sntp

sntp authentication-key

sntp—enable/disable

sntp server

sntp set poll-interval

sntp

Use this command to enter SNTP configuration mode.

Command mode

Global configuration

Syntax

```
sntp
```

Related commands

`show sntp status`

sntp authentication-key

Use this command to set the authentication parameters. Precede this command with no to disable authentication.

Command mode

SNTP configuration

Syntax

```
sntp authentication-key <key-id> {MD5} <key>


no sntp authentication
```

Variable definitions

This table describes the variables used in the `sntp authentication-key` command.

Variable	Value
key-id	Specifies the Key Identifier (integer value). The value ranges from 1 to 65535.
MD5	Specifies the message digest algorithm.
key	Specifies the key value (string value).

Related commands

`show sntp status`

sntp—enable/disable

Use this command to start or stop the SNTP client.

Command mode

SNTP configuration

Syntax

```
sntp {enable | disable}
```

Variable definitions

This table describes the variables used in the `sntp—enable/disable` command.

Variable	Value
enable	Starts the SNTP client.
disable	Stops the SNTP client.

Related commands

`show sntp status`

sntp no time zone

Use this command to reset system time zone to GMT. It resets the time zone difference to + 00:00 (Forward Time Zone Hours:Minutes).

Command mode

SNTP configuration

Syntax

```
sntp no time zone
```

Related commands

`show sntp clock`

sntp server

Use this command to specify the IP address of the SNTP server.

Command mode

SNTP configuration

Syntax

```
sntp server <server-ip>
```

Variable definitions

This table describes the variables used in the **sntp server** command.

Variable	Value
server-ip	Server IP address.

Related commands

`show sntp status`

sntp set poll-interval

Use this command to set the poll interval value in seconds.

Command mode

SNTP configuration

Syntax

```
sntp set poll-interval <number(4-14)>
```

Variable definitions

This table describes the variables used in the **sntp set poll-interval** command.

Variable	Value
number	Poll interval value in seconds.

Related commands

show sntp status

sntp time zone

Use this command to set the system time zone with respect to Greenwich Mean Time (GMT).

Command mode

SNTP configuration

Syntax

```
sntp time zone <+/-> <UTC TimeDiff in Hrs> <UTC TimeDiff in Min>
```

Variable definitions

This table describes the variables used in the **sntp time zone** command.

Variable	Value
+/-	After or before UTC.
UTC TimeDiff in Hrs	UTC time difference in hours.
UTC TimeDiff in Min	UTC time difference in minutes.

Related commands

`show sntp clock`

Network Address Translation commands

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the internet, without requiring a registered subnet address. This eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

With NAT, the privately addressed network (designated as inside) continues to use its existing private or obsolete addresses. These addresses are converted into legal addresses before packets are forwarded onto the registered network (designated as outside). The translation function is compatible with standard routing; the feature is required only on the router connecting the inside network to the outside domain.

NAT command navigation

- debug nat (page 653)
- enable virtual server (page 655)
- interface nat (page 656)
- ip nat (page 657)
- ip nat pool (page 658)
- ip nat—timeout (page 659)
- no virtual server (page 660)
- port trigger (page 662)
- show ip nat (page 663)
- show ip nat interface (page 664)
- show nat config (page 665)
- show portrange (page 666)
- show port trigger (page 667)
- show port trigger reserved list (page 668)
- show virtual servers (page 669)
- static nat (page 670)
- virtual server (page 671)

debug nat

Use this command to set the NAT module trace level. Precede this command with `no` to reset the NAT module trace level.

Command mode

Privileged Exec

Syntax

```
debug nat [all] [fn-entry] [fn-exit] [packet-flow] [dns] [ftp] [http]
[smtp] [icmp] [pptp] [memory]


no debug nat [all] [fn-entry] [fn-exit] [packet-flow] [dns] [ftp] [http]
[smtp] [icmp] [pptp] [memory]
```

Variable definitions

This table describes the variables used in the `debug nat` command.

Variable	Value
all	Specifies all traces.
fn-entry	Specifies the function entry related traces.
fn-exit	Specifies the function exit related traces.
packet-flow	Specifies the packet-flow related traces.
dns	Specifies the DNS related traces.
ftp	Specifies the FTP related traces.
http	Specifies the HTTP related traces.
smtp	Specifies the SMTP related traces.
icmp	Specifies the ICMP related traces.
pptp	Specifies the PPTP related traces.
memory	Specifies the memory related traces.

Defaults

```
disabled
```

disable virtual server

Use this command to disable the virtual server configuration.

Command mode

Interface configuration

Syntax

```
disable virtual server {{<local ip> <port number>} | all}
```

Variable definitions

This table describes the variables used in the `disable virtual server` command.

Variable	Value
local ip	Enter the local IP address.
port number	Enter the port number.
all	Specifies all virtual servers.

Related commands

`interface nat`

`ip nat–timeout`

`virtual server`

enable virtual server

Use this command to enable the virtual server configuration.

Command mode

Interface configuration

Syntax

```
enable virtual server {{<local ip> <portno>} | all}
```

Variable definitions

This table describes the variables used in the `enable virtual server` command.

Variable	Value
local ip	Enter local IP address.
portno	Enter the port number.
all	Specifies all virtual servers.

Related commands

`interface nat`

`ip nat–timeout`

`virtual server`

interface nat

Use this command to enable or disable interface NAT status.

Command mode

Interface configuration

Syntax

```
interface nat {enable | disable}
```

Variable definitions

This table describes the variables used in the `interface nat` command.

Variable	Value
enable	Enable interface NAT status.
disable	Disable interface NAT status.

Defaults

Disabled

Related commands

`ip nat`

`show ip nat interface`

ip nat

Use this command to enable NAT. Precede this command with no to disable NAT.

Command mode

Global configuration

Syntax

```
ip nat
no ip nat
```

Related commands

show nat config

ip nat pool

Use this command to add global address pools. Precede this command with no to delete global address pools.

Command mode

Interface configuration

Syntax

```
ip nat pool <global ip> <mask>

no ip nat pool <global ip>
```

Variable definitions

This table describes the variables used in the `ip nat pool` command.

Variable	Value
global ip	Specifies the global IP address.
mask	Specifies the subnet mask.

Related commands

`show ip nat`

ip nat—timeout

Use this command to configure the Network Address Translation (NAT) value.

Command mode

Global configuration

Syntax

```
ip nat { idle | tcp | udp } timeout <seconds (60 - 86400)>
```

Variable definitions

This table describes the variables used in the `ip nat—timeout` command.

Variable	Value
idle	Specifies the NAT idle timeout value in seconds.
tcp	Specifies the NAT TCP timeout value in seconds.
udp	Specifies the NAT UDP timeout value in seconds.
timeout	Specifies the NAT timeout value in seconds.

Defaults

idle	60 seconds
tcp	86400 seconds
udp	300 seconds

Related commands

`show nat config`

no virtual server

Use this command to delete the virtual server configuration. WAN interface must be created before the execution of this command. For deleting virtual server 5060 for tcp entry, it is recommended to use optional protocol field. For example, no virtual server 192.168.1.1 5060 tcp.

Command mode

Interface configuration

Syntax

```
no virtual server { { <local ip> <local port number> [<tcp|udp|any>] } |
all }
```

Variable definitions

This table describes the variables used in the `no virtual server` command.

Variable	Value
local ip	Specifies the local IP address for the virtual server.
local port number	Specifies the local port number for the virtual server.
tcp|udp|any	Specifies the transport protocols.
all	Specifies all virtual servers.

Related commands

`virtual server`

portrange

Use this command to configure the port forwarding range. Precede this command with no to delete the port forwarding range.

Command mode

Interface configuration

Syntax

```
portrange <local ip> {tcp|udp|any} <start port no> <end port no>

no portrange <local ip> {tcp|udp|any} <start port no><end port no>
```

Variable definitions

This table describes the variables used in the `portrange` command.

Variable	Value
local ip	Specifies the local IP address.
tcp|udp|any	Specifies the protocol name.
start port no	Specifies the start port number.
end port no	Specifies the end port number.

Related commands

`show portrange`

port trigger

Use this command to configure port trigger for outbound and inbound application. Precede this command with no to delete the configured port trigger for the given application.

Command mode

Interface configuration

Syntax

```
port trigger <App Name> {tcp|udp|any} <Outbound Port Range> <Inbound
Port Range>


no port trigger <App Name>
```

Variable definitions

This table describes the variables used in the `port integer` command.

Variable	Value
App Name	Specifies the application name.
tcp|udp|any	Specifies the protocol name.
Outbound Port Range	Specifies the outbound port range.
Inbound Port Range	Specifies the inbound port range.

Related commands

`show port trigger`

`show port trigger reserved list`

show ip nat

Use this command to display various NAT tables.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip nat {global | static | translations}
```

Variable definitions

This table describes the variables used in the `show ip nat` command.

Variable	Value
global	Specifies the global IP NAT.
static	Specifies the static IP NAT.
translations	Specifies the NAT.

Related commands

`static nat`

`ip nat pool`

show ip nat interface

Use this command to display NAT interface configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ip nat interface
```

Related commands

interface nat

ip nat

show nat config

Use this command to display NAT configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show nat config
```

Related commands

`static nat`

show portrange

Use this command to display the port range configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show portrange
```

Related commands

show portrange

show port trigger

Use this command to display the port trigger configurations.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show port trigger
```

Related commands

port trigger

show port trigger reserved list

Use this command to display the port trigger reserved list.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show port trigger reserved list
```

Related commands

port trigger

show virtual servers

Use this command to display the current virtual server configurations.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show virtual servers
```

Related commands

`virtual server`

static nat

Use this command to add a static mapping between local and global address on the specified interface. Precede this command with no to delete the static mapping for the given local IP on the specified interface.

Command mode

Interface configuration

Syntax

```
static nat <local ip> <translated local ip>
no static nat <local ip>
```

Variable definitions

This table describes the variables used in the `static nat` command.

Variable	Value
local ip	Local IP address.
translated local ip	Translated local IP address.

Related commands

`show ip nat`

virtual server

Use this command to configure a virtual server. Precede this command with no to delete the virtual server configuration.

Command mode

Interface configuration

Syntax

```
virtual server <localip> [<local port number>] {auth | dns | ftp | pop3 |
pptp | smtp | telnet | http | nntp | snmp | other} [<global port number>]
} } [<tcp|udp|any>] [<description>]


no virtual server {{<local ip> <local port number>} | all}
```

Variable definitions

This table describes the variables used in the `virtual server` command.

Variable	Value
local ip	Specifies the local IP address for the virtual server.
local port number	Specifies the local port number for the virtual server.
auth | dns | ftp | pop3| pptp | smtp | telnet| http | nntp |snmp|other	Specifies the application mode for the virtual server.
global port number	Specifies the external port number for the virtual server.
tcp|udp|any	Specifies the transport protocols.
description	Specifies the description of the internal host.
all	Specifies all virtual servers.

Related commands

`show virtual servers`

Virtual private network policy commands

The Virtual Private Network (VPN) policy commands are used to configure remote access with IPSec or Layer 2 Tunneling Protocol (L2TP). A VPN is a private communications network used by companies or organizations, to communicate confidentially over a public network. VPN traffic is carried over a public networking infrastructure.VPN connections are more cost-effective than dedicated private lines.

VPN supports Internet Protocol Security (IPSec) and Internet Key Exchange (IKE).

VPN policy commands navigation

- access list (page 673)
- clear vpn logs (page 674)
- crypto key mode (page 676)
- crypto map (page 677)
- crypto map - Interface (page 678)
- crypto map ipsec (page 679)
- ip ra-vpn pool (page 680)
- isakmp peer identity (page 681)·
- isakmp policy encryption (page 682)
- ra-vpn username (page 683)
- set local identity (page 684)
- set peer (page 685)
- set session key (page 686)
- set vpn (page 687)
- show crypto map (page 688)
- show ra-vpn users (page 689)
- show ra-vpn address-pool (page 690)
- show vpn config (page 691)
- show vpn global statistics (page 692)
- show vpn IKE statistics (page 693)
- show vpn logs (page 694)
- show vpn remote—ids (page 695)
- vpn remote identity (page 696)

access list

This command specifies the source and destination IP address to which the policy is applied with the type of traffic and action to be taken.

Command mode

Crypto Map Configuration

Syntax

```
access-list {permit|deny|apply} {any|tcp|udp|icmpv4|ahproto|espproto}
source <ip-address> <subnet-mask> destination <ip-addrress>
<subnet-mask>
```

Variable definitions

This table describes the variables used in the `access-list` command.

Variable	Value
permit|deny|apply	Permit or Deny or Apply the Access list
any|tcp|udp|icmpv4|ahproto|espproto	Any protocol or TCP protocol or UDP protocol or ICMPv4 protocol or AH protocol or ESP protocol
source <ip-address>	Source IP Address
source <subnet-mask>	Source IP Subnet Mask
destination <ip-addrress>	Destination IP Address
destination <subnet-mask>	Destination IP Subnet Mask

clear vpn logs

This command clears the log file contents of the VPN subsystem.

Command mode

Privileged/User Exec

Syntax

```
clear vpn logs
```

crypto ipsec mode

Use this command to configure the IPSEC mode.

Command mode

Crypto Map Configuration

Syntax

```
crypto ipsec mode {tunnel | transport}
```

Variable definitions

This table describes the variables used in the `crypto ipsec mode` command.

Variable	Value
tunnel	Specifies the tunnel Mode
transport	Specifies the transport Mode

crypto key mode

Use this command to specify the type of VPN used.

Command mode

Crypto Map Configuration

Syntax

```
crypto key mode {ipsec-manual | preshared-key | cert | xauth |
ravpn-preshared-key}
```

Variable definitions

This table describes the variables used in the `crypto key mode` command.

Variable	Value
ipsec-manual	Specifies manual IPSEC.
preshared-key	Specifies the preshared Key
xauth	Specifies the extended authentication
cert	Specifies the certificate
ravpn-preshared-key	Specifies the authentication mode specific to RA VPN policy. In this mode, authentication is done with preshared key only (without user authentication).

crypto map

This command creates a new crypto map which will define the VPN policy to be negotiated for SA creation.

Command mode

Global Configuration

Syntax

```
crypto map <policy-name>


no crypto map {<map-name> | all}
```

Variable definitions

This table describes the variables used in the `crypto map` command.

Variable	Value
policy-name	Name of the crypto map to be created.
map- name	Specified Crypto map name.
all	All the policies.

crypto map - Interface

This command applies the crypto policy to the specified interface. Precede this command with no to disable the policy applied to the specific interface.

Command mode

Interface Configuration

Syntax

```
crypto map <policy name>


no crypto map <policy-name>
```

Variable definitions

This table describes the variables used in the `crypto map` command.

Variable	Value
policy-name	Specifies the policy name.

crypto map ipsec

Use this command to specify the IKE Phase II Proposal with encryption and authenitication algorithm, mode of transaction and lifetime as parameters.

Command mode

Crypto Map Configuration

Syntax

```
crypto map ipsec {[encryption esp {null | des | triple-des | aes |aes-192
| aes-256}] [authentication {esp | ah} {md5 | sha1}]}[pfs {group1 |
group2 | group5}][lifetime {secs | mins | hrs | days} <lifetime>]
```

Variable definitions

This table describes the variables used in the `crypto map ipsec` command.

Variable	Value
encryption esp {null|des| triple-des|aes|aes-192|aes-256}	Specifies the encryption algorithm.
authentication {esp|ah}	Authentication algorithm – can be either Encapsulating security Payload or Authentication Header.
md5 | sha1	Specifies the authentication algorithm which can be either md5 or sha1.
pfs {group1|group2|group5}	Specifies the IKE group 1 or 2 or 3.
lifetime(sec|min|hrs|days)	Specifies the lifetime.

ip ra-vpn pool

Use this command to configure the IP address pool for assigning IP addresses for remote users. Precede this command with `no` to delete the IP address pool for remote users.

Command mode

Global Configuration

Syntax

```
ip ra-vpn pool <poolname> <start_ip> - <end_ip>


no ip ra-vpn pool <poolname>
```

Variable definitions

This table describes the variables used in the `ip ra-vpn pool` command.

Variable	Value
poolname	Specifies the IP Address pool name which is a string of length from 1 to 32.
start ip-end-ip	Specifies the range of the IP address. The start and end IP must belong to the same subnet.

isakmp peer identity

Use this command to configure the peer identity type and its value to be used in IKE Phase 1. It can be IP address, email, fqdn or key id.

Command mode

Crypto map configuration

Syntax

```
isakmp peer identity {ipv4|email|fqdn|keyId} <id-value>
```

Variable definitions

This table describes the variables used in the `isakmp peer identity` command.

Variable	Value
ipv4 | email | fqdn | keyId	Identitifies the peer type as follows: IPv4 Address E-mail address Fully Qualified Domain Name String
id-value-	Identity value corresponding to the selected Identity.

isakmp policy encryption

Use this command to specify the IKE Phase I proposal with encryption and authenitication algorithm, mode of transaction, and lifetime as parameters.

Command mode

Crypto map configuration

Syntax

```
isakmp policy encryption {des | triple-des | aes | aes-192 | aes-256}
hash {md5 | sha1} dh {group1|group2|group5} exch {main|aggressive}
lifetime {secs|mins|hrs} <lifetime>
```

Variable definitions

This table describes the variables used in the `isakmp policy encryption` command.

Variable	Value
des| triple-des | aes | aes-192| aes-256	Specifies the encryption algorithm.
md5 | sha1	Specifies the authentication algorithm .It can be either md5 or sha1.
group1|group2|group5	Specifies the IKE group 1 or 2 or 3.
main|aggressive	Specifies the IKE exchange mode.
lifetime(sec|min|hrs)	Specifies the duration of the lifetime in sec/min/hrs.
lifetime	Specifies the lifetime value in selected time unit in sec|min|hrs.

ra-vpn username

Use this command configures usernames and password to identify remote access users to the device and the no form of this command deletes the existing users from accessing Remote Acess VPN.

Command mode

Global Configuration

Syntax

```
ra-vpn username <username> password <password>


no ra-vpn username <username>
```

Variable definitions

This table describes the variables used in the `ra-vpn username` command.

Variable	Value
username	Specifies the user name. User name can be alphanumeric characters of length 1 to 32.
password	Specifies the password. Password can be alphanumeric characters of length 1 to 32.

set local identity

This command configures the local identity type and its value to be used in IKE Phase 1. It can be IP address, email, fqdn, or key id.

Command mode

Crypto Map Configuration

Syntax

```
set local identity {ipv4|email|fqdn|keyId} <id-value>
```

Variable definitions

This table describes the variables used in the `set local identity` command.

Variable	Value
ipv4 | email | fqdn | keyId	Identitifies the local identity type, which are as follows: • IPv4 Address • E-mail address • Fully Qualified Domain Name • String
id-value	Specifies the iIdentity value corresponding to the selected Identity.

set peer

Use this command to set the destination address in the packet during authentication and encryption of outbound datagrams.

Command mode

Crypto Map Configuration

Syntax

```
set peer <peer-ip>
```

Variable definitions

This table describes the variables used in the `set peer` command.

Variable	Value
peer-ip	Destination Address

set session key

This command specifies the mode of VPN along with the authentication and encryption algorithm with inbound and outbound SPI.

Command mode

Crypto Map Configuration

Syntax

```
set session-key {[authenticator {ah | esp} {hmac-md5 |
hmac-sha1}<auth-key>] [esp {des cipher <key> |triple-des cipher <key1>
<key2> <key3> | {aes |aes-192 |aes-256} cipher <key>}]} outbound <spi
(256-2147483647)>inbound <spi (256-2147483647)> [anti-replay]
```

Variable definitions

This table describes the variables used in the `set session-key` command.

Variable	Value
authenticator {ah | esp}	Authenticator – can be either of the following: ah - Authenticator with Authentication Header esp - Authenticator with Encapsulating Security Payload
hmac-md5|hmac-sha1	Authentication algorithms
auth key	Authentication Key
des cipher	Encapsulating Security Payload with DES algorithm
triple-des cipher	Encapsulating Security Payload with Triple DES algorithm
aes-128	Encapsulating Security Payload with AES-128 algorithm
aes-19	Encapsulating Security Payload with AES-192 algorithm
aes-256	Encapsulating Security Payload with AES-256 algorithm
outbound	Outbound Security Parameter Index
inbound	Inbound Security Parameter Index
anti-replay	Anti Replay

set vpn

This command enables or disables the VPN module for encryption and decryption of the flows.

Command mode

Global Configuration

Syntax

```
set vpn {enable | disable}
```

Variable definitions

This table describes the variables used in the `set vpn` command.

Variable	Value
enable	Enables the VPN module.
disable	Disables the VPN module.

show crypto map

Use this command to display the crypto policy parameters of the specified interface.

Command mode

Privileged EXEC or User EXE

Syntax

```
show crypto map [<policy name>]
```

Variable definitions

This table describes the variables used in the `show crypto map` command.

Variable	Value
policy name	Specifies the policy name.

show ra-vpn users

Use this command to display the user information configured to do remote access.

Command mode

Privileged EXEC orUser EXEC

Syntax

```
show ra-vpn users
```

show ra-vpn address-pool

Use this command to display the IP address pool assigned for remote users.

Command mode

Privileged EXEC orUser EXEC

Syntax

```
show ra-vpn address-pool
```

show vpn config

This command displays the global VPN settings.

Command mode

Privileged EXEC orUser EXEC

Syntax

```
show vpn config
```

show vpn global statistics

Use this command to display the in, out, secured and dropped packet in the VPN module.

Command mode

Privileged or user EXEC

Syntax

```
show vpn global statistics
```

show vpn IKE statistics

Use this command to display the IKE and IPSec Security Associations (SA) statistics.

Command mode

Privileged or user EXEC

Syntax

```
show vpn ike statistics
```

show vpn logs

Use this command to display the last N pages of the VPN log file from the VPN processor.

Command mode

Privileged or user EXEC

Syntax

```
show vpn logs [page-count <num_pages>]
```

Variable definitions

This table describes the variables used in the `show vpn logs` command.

Variable	Value
page-count	Specifies the number of pages to display at a time.

show vpn remote—ids

Use this command to display the VPN remote identities existing in the system. For instance, you specify the ipv4 as a remote identity type, all the ipv4 identities are displayed.

Command mode

Privileged or user EXEC

Syntax

```
show vpn remote-ids [ipv4 | fqdn | email | key-id]
```

Variable definitions

This table describes the variables used in the `show vpn remote—ids` command.

Variable	Value
ipv4	Specifies the IPv4 address.
email	Specifies the e-mail address.
fqdn	Specifies the fully qualified domain name.
keyId	Specifies the string to uniquely identify the peer.

vpn remote identity

Use this command to configure the remote identity information. It is a preshared key. Precede this command with `no` to delete the remote identify and its preshared key mappings.

Command mode

Global configuration

Syntax

```
vpn remote identity {ipv4 | email | fqdn | keyId} <id-value> psk
<preshared-key>


no vpn remote identity {ipv4 | email | fqdn | keyId} <id-value>
```

Variable definitions

This table describes the variables used in the `vpn remote identity` command.

Variable	Value
ipv4	Specifies the IPv4 address.
email	Specifies the e-mail address.
fqdn	Specifies the fully qualified domain name.
keyId	Specifies the string to uniquely identify the peer.
psk	Specifies the preshared key.

Related commands

`show vpn remote—ids`

Diffserv commands

Differentiated Services (DiffServ) is an architecture for providing different types or levels of services for network traffic. In Diffserv, flows are aggregated in the network so that the core routers can distinguish small aggregated flows that contain million of individual flows.

Differentiated services provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services speeds the deployment by dividing the architecture into two components, one is well understood and other is just beginning to be understood. This decision is taken from the internet design, which separates the forwarding and routing components. Packet forwarding is a relatively simple task that performs on a per-packet basis. Forwarding uses the packet header to find an entry in a routing table that determines the packet's output interface. Routing sets the entries in that table and reflects a range of transit and other policies to keep track of route failures. Routing tables act as a background process to the forwarding task.

Diffserv commands navigation

- class (page 698)
- class-map (page 699)
- no policy-map (page 701)
- police (page 702)
- policy-map (page 703)
- queue threshold (page 704)
- queue weight (page 705)
- set qos (page 706)
- set vlan traffic-classes (page 707)
- show class-map (page 708)
- show policer statistics (page 709)
- show policy-map (page 710)
- show qos default dhcp-dot1p mapping (page 711)
- show qos status (page 712)
- show queue stats (page 713)
- show queuing (page 714)
- show vlan port config (page 715)
- show vlan traffic-classes (page 716)
- shutdown qos (page 717)
- switchport priority default (page 718)
- vlan map—priority (page 719)
- vlan max-traffic-class (page 720)

class

Use this command to set the priority and Differentiated Services Code Point (DSCP) values in the classifier.

Command mode

Global configuration

Syntax

```
class <classifier-id> [set ip dscp <dscp value> ] [priority <priority value> ]
```

Variable definitions

This table describes the variables used in the `class` command.

Variable	Value
classifier-id	Specifies Class ID. The value ranges from 1 to 2147483647.
dscp value	Specifies Differentiated Services Code Point (DHCP) value. The value ranges from 0 to 63.
priority value	Specifies the priority value assigned to the classified traffic. The value ranges from 0 to 7.

Related commands

`show class-map`

`show policy-map`

class-map

Use this command to create a multi field classifier. Precede this command with `no` to delete the classifier entry.

Command mode

Global configuration

Syntax

```
class-map <classifier-id> [permit[{tcp|udp}] [{source-host <source
address>|source-net<source network> <source mask>}] [{dest-host
<destination address>| dest-net <destination network> <destination mask
>}] [source-port <source port>] [dest-port <destination port>] [dscp
<dscp value>] [interface {<Interface Type> <Interface Index> | vlan
<vlan id>}]]


no class-map <classifier-id>
```

Variable definitions

This table describes the variables used in the `class-map` command.

Variable	Value
classifier-id	Specifies class identifier. The value ranges from 1 to 2147483647.
permit	Allows the TCP / UDP packets to be forwarded.
source-host	Specifies the source Host address.
source-net	Specifies the source network address.
dest-host	Specifies the destination host address.
dest-net	Specifies the destination network address.
source-port	Specifies the source port. The value ranges from 1 to 65535.
dest-port	Specifies the destination port. Value r anges from 1 to 65535
dscp	Specifies the incoming diffserv code point (DSCP) value.
interface Type	Type of the Ingress L3 Interface. This interface can be either virtual interface or router port.
interface Index	Specifies the value of the interface index.
vlan id	Specifies the VLAN identifier. The value ranges from 1 to 4094.

Related commands

show class-map

class

no policy-map

This command deletes the policer entry.

Command mode

Global configuration

Syntax

```
no policy-map <policer-id>
```

Variable definitions

This table describes the variables used in the `no policy-map` command.

Variable	Value
policer-id	Specifies Policer Identifier. The value ranges from 1 to 2147483647.

Related commands

`show policy-map`

`police`

police

Use this command to create a policer entry.

Command mode

Global configuration

Syntax

```
police <policer-id> [type {trtcm}]  [ PIR < Peak Information Rate - bytes
per second, MAX value: 133000000> ]  [CIR <Committed Information Rate -
Bytes per second, MAX value: 133000000> ] [PBS <Peak Burst Size - In
Bytes>]  [CBS <Committed Burst Size - Bytes>]
```

Variable definitions

This table describes the variables used in the `police` command.

Variable	Value
policer-id	Specifies policer identifier. Value ranges from 1 to 2147483647.
type	Specifies the policer type.
PIR	Specifies Peak Information Rate (PIR) value in bytes per second.
CIR	Specifies Committed Information Rate (CIR) value in bytes per second.
PBS	Specifies Peak Burst Size (PBS) in bytes.
CBS	Specifies Committed Burst Size (CBS) in bytes.

Defaults

Policer Type	trtcm
PBS	2000
CBS	1500
PIR	3250000
CIR	3000000

Related commands

`no policy-map`

`policy-map`

`show class-map`

`show policy-map`

policy-map

Use this command to map a classifier entry with the appropriate policer.

Command mode

Global configuration

Syntax

```
policy-map <policer id> class <classifier id>
```

Variable definitions

This table describes the variables used in the `policy-map` command.

Variable	Value
policer id	Specifies the value of the policer ID. The value ranges from 1 to 2147483647.
classifier id	Specifies the value for the classifier ID. The value ranges from 1 to 2147483647.

Related commands

`police`

`class-map`

queue threshold

Use this command to configure the RED parameters of a queue.

Command mode

Interface configuration

Syntax

```
queue threshold <queue-number> <min-green-threshold - 256 byte blocks>
<max- green-threshold - 256 byte blocks> <min-amber-threshold - 256 byte
blocks> <max-amber-threshold - 256 byte blocks>
```

Variable definitions

This table describes the variables used in the `queue threshold` command.

Variable	Value
queue-number	Specifies the value for the queue number.
min-green-threshold	Specifies the minimum green threshold value.
max- green-threshold	Specifies the maximum green threshold value.
min-amber-threshold	Specifies the minimum amber threshold value.
max-amber-threshold	Specifies the maximum amber threshold value.

queue weight

Use this command to configure the weight of a queue. Configure the weight to zero to make the queue to be a part of strict priority scheduler.

Command mode

Interface Configuration

Syntax

```
queue weight <queue-number> <queue-weight>
```

Variable definitions

This table describes the variables used in the `queue weight` command.

Variable	Value
queue-number	Specifies the value for queue number.
queue-weight	Specifies the value for queue weight.

set qos

Use this command to configure the control status of the Diffserv system.

Command mode

Global Configuration

Syntax

```
set qos { enable | disable }
```

Variable definitions

This table describes the variables used in the `set qos` command.

Variable	Value
enable	Enables differentiated services.
disable	Disables differentiated services.

Defaults

enable

Related commands

`show qos status`

`shutdown qos`

set vlan traffic-classes

Use this command to enable or disable traffic classes.

Command mode

Global configuration

Syntax

```
set vlan traffic-classes {enable | disable}
```

Variable definitions

This table describes the variables used in the `set vlan traffic-classes` command.

Variable	Value
enable	Enables traffic classes.
disable	Disables traffic classes.

Defaults

`enable`

Related commands

`show vlan`

`show vlan traffic-classes`

`switchport priority default`

show class-map

Use this command to display one or more classifiers information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show class-map [<classifier-id>]
```

Variable definitions

This table describes the variables used in the `show class-map` command.

Variable	Value
classifier-id	Specifies the value of the classifier ID. The value ranges from 1 to 2147483647.

Related commands

`class-map`

`class`

show policer statistics

Use this command to display one or more information of policers statistics .

Command mode

Privileged EXEC or User EXEC

Syntax

```
show policer statistics [<policer-id (1-2147483647)>]
```

Variable definitions

This table describes the variables used in the `show policer statistics` command.

Variable	Value
policer-id	Specifies the value of the policer ID. Value ranges from 1 to 2147483647.

Related commands

`police`

`policy-map`

show policy-map

Use this command to display one or more policers information.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show policy-map  [<policer-id>]
```

Variable definitions

This table describes the variables used in the `show policy-map` command.

Variable	Value
policer-id	Specifies the value of the policer ID. The value ranges from 1 to 2147483647.

Related commands

`set qos`

`class-map`

`police`

`no policy-map`

`policy-map`

`shutdown qos`

show qos default dhcp-dot1p mapping

Use this command to display the default mapping of DHCP to 802.1p user priorities. The default DSCP to 802.1p mapping cannot be modified by the user.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show qos default dscp-dot1p mapping
```

show qos status

Use this command to display the status of the QoS module.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show qos status
```

show queue stats

Use this command to display the queue statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show queue stats [interface <Type> <Number> [queue <(0-7)>]]
```

Variable definitions

This table describes the variables used in the `show queue stats` command.

Variable	Value
interface	Specifies the interface type and number.
queue	Specifies the queue number. The value ranges from 0 to 7.

Related commands

`set qos`

`shutdown qos`

show queuing

Use this command to display one or more queue information.

Command mode

Privileged EXEC orUser EXEC

Syntax

```
show queuing [{strict-priority | random-detect | Weighted-Round-Robin}]
[interface <interface-type> <interface-no>]
```

Variable definitions

This table describes the variables used in the `show queuing` command.

Variable	Value
strict-priority	Specifies strict priority queue information.
random-detect	Specifies random detect queue information.
Weighted-Round-Robin	Displays weighted round robin queue information.
interface-type	Enter the type of interface.
interface-no	Enter the interface number.

Related command

`queue threshold`

`queue weight`

show vlan port config

Use this command to display the VLAN-related parameters specific for ports.

Command mode

Privileged EXEC orUser EXEC

Syntax

```
show vlan port config [{port <interface-type> <interface-id> }]
```

Variable definitions

This table describes the variables used in the `show vlan port config` command.

Variable	Value
port	Specifies the interface ID and interface type of the VLAN.

Related commands

show firewall config

show firewall interface config

show nat config

show vpn config

show vlan traffic-classes

Use this command to display the traffic classes information of all the available interfaces.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show vlan traffic-classes [{port <interface-type> <interface-id>}]
```

Variable definitions

This table describes the variables used in the `show vlan traffic-classes` command.

Variable	Value
port	Specifies the interface type and port ID of the port.

Related commands

`ports`

`set vlan traffic-classes`

`vlan`

`switchport priority default`

shutdown qos

Use this command to shut down Quality-of-Service (QoS) operation. Precede this command with `no` to start and enable the QoS operation.

Command mode

Global configuration

Syntax

```
shutdown qos
```

```
no shutdown qos
```

Defaults

QoS is started and enabled

Related commands

switchport priority default

Use this command to configure the default user priority for the port. Precede this command with no to configure the default user priority for the port to the default value to a port.

Command mode

Interface configuration

Syntax

```
switchport priority default <priority value(0-7)>


no switchport priority default
```

Defaults

0

Related commands

`show vlan port config`

vlan map—priority

Use this command to map a priority to a traffic class on the specified port. The frame received on the interface with the configured priority is processed in the configured traffic class. Precede this command with no to map the default priority to traffic class value on the port.

Command mode

Interface configuration

Syntax

```
vlan map—priority <priority value(0-7)> traffic-class <Traffic class value(0-7)>


no vlan map-priority <priority value (0-7)>
```

Variable definitions

This table describes the variables used in the `vlan map—priority` command.

Variable	Value
Traffic class	Specifies the traffic classes supported on the port.

Related commands

`show vlan traffic-classes`

vlan max-traffic-class

Use this command to configure the maximum number of traffic classes supported on a port. Precede this command with no to assign the default maximum traffic class value to a port.

Command mode

Interface configuration

Syntax

```
vlan max-traffic-class <MAX Traffic class(1-8)>


no vlan max-traffic-class
```

Variable definitions

This table describes the variables used in the `vlan max-traffic-class` command.

Variable	Value
MAX Traffic class	Specifies the number of traffic classes supported on the port.

Defaults

8

Related commands

`show vlan traffic-classes`

Access control list commands

Access Control Lists (ACL) filters the network traffic by controlling whether routed packets are forwarded or blocked at the router interfaces. ACLs block IP packets from being forwarded by a router. The router examines each packet to determine whether to forward or drop the packet, based on the criteria specified within the access lists.

ACL navigation

- deny (page 722)
- mac access-group (page 724)
- mac access-list extended (page 725)
- permit (page 726)
- show access-lists (page 728)

deny

Use this command to specify the packets to reject based on the MAC address and the associated parameters.

Command mode

ACL MAC configuration

Syntax

```
deny { any | host <mac-address>}{ any | host <mac-address> } [aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)>] [ encaptype <value (1-65535)>][ Vlan <vlan-id (1-4094)>] [priority <value (1-255)>]
```

Variable definitions

This table describes the variables used in the `deny` command.

Variable	Value
any | host <mac_addr>	Specifies the source MAC address to match with the packet.
any | host <mac_addr>	Specifies the destination MAC address to match with the packet.
aarp	Specifies the Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	Specifies the EtherType DEC-Amber.
dec-spanning	Specifies the EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	Specifies the EtherType DECnet Phase IV protocol.
diagnostic	Specifies the EtherType DEC-Diagnostic.
dsm	Specifies the EtherType DEC-DSM/DDP.
etype-6000	Specifies the EtherType 0x6000.
etype-8042	Specifies the EtherType 0x8042.
lat	Specifies the EtherType DEC-LAT.
lavc-sca	Specifies the EtherType DEC-LAVC-SCA.
mop-console	Specifies the EtherType DEC-MOP Remote Console.
mop-dump	Specifies the EtherType DEC-MOP Dump.
msdos	Specifies the EtherType DEC-MSDOS.
mumps	Specifies the EtherType DEC-MUMPS.

Variable	Value
netbios	Specifies the EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	Specifies the Ether type Virtual Integrated Network Service (VINES) Echo from Banyan systems.
vines-ip	Specifies the Ether type VINES IP.
xns-id	Specifies the Ether type Xerox Network Systems (XNS) protocol suite identifier.
encaptype	Specifies the encapsulation type.
vlan	Specifies the VLAN ID to be filtered.
priority	Specifies the priority of the L2 filter, which is used to decide the applicable rule when the packet matches more than one filter rule. Higher value of filter priority implies a higher priority.

Defaults

vlan-id	0
priority	1

Related commands

mac access-group

mac access-list extended

permit

`show access-lists`

mac access-group

Use this command to apply a MAC ACL to a Layer 2 interface. Precede this command with `no` to remove the MAC ACLs from the interface.

Command mode

Interface configuration

Syntax

```
mac access-group <access-list-number (1-65535)> in


no mac access-group [<access-list-number (1-65535)>] in
```

Variable definitions

This table describes the variables used in the `mac access-group` command.

Variable	Value
access list number	Specifies the access list number.
in	Specifies the inbound packets.

Related commands

deny

mac access-list extended

permit

show access-lists

mac access-list extended

Use this command to create the Layer 2 MAC ACLs. This command creates a MAC ACL and returns the MAC ACL configuration mode to the user. Precede this command with `no` to delete the MAC ACL.

Command mode

Global configuration

Syntax

```
mac access-list extended <access-list-number (1-65535)>


no mac access-list extended <short (1-65535)>
```

Variable definitions

This table describes the variables used in the `mac access-list extended` command.

Variable	Value
access-list-number	Specifies the access list number.

Related commands

deny

mac access-group

show access-lists

permit

permit

Use this command to specify the forwarded packets based on the MAC address and the associated parameters. This command allows non-IP traffic to be forwarded if the conditions are matched.

Command mode

ACL MAC configuration

Syntax

```
permit { any | host <mac-address>}{ any | host <mac-address> }
[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000
|etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps
| netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)>]
[ encaptype <value (1-65535)>][ Vlan <vlan-id (1-4094)>][priority <value
(1-255)>]
```

Variable definitions

This table describes the variables used in the `permit` command.

Variable	Value
any | host <mac_addr>	Specifies the source MAC address to match with the packet.
any | host <mac_addr>	Specifies the destination MAC address to match with the packet.
aarp	Specifies the Ethertype AppleTalk Address Resolution Protocol mapping a data-link address to a network address.
amber	Specifies the EtherType DEC-Amber.
dec-spanning	Specifies the EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	Specifies the EtherType DECnet Phase IV protocol.
diagnostic	Specifies the EtherType DEC-Diagnostic.
dsm	Specifies the EtherType DEC-DSM/DDP.
etype-6000	Specifies the EtherType 0x6000.
etype-8042	Specifies the EtherType 0x8042.
lat	Specifies the EtherType DEC-LAT.
lavc-sca	Specifies the EtherType DEC-LAVC-SCA.
mop-console	Specifies the EtherType DEC-MOP Remote Console.
mop-dump	Specifies the EtherType DEC-MOP Dump.
msdos	Specifies the EtherType DEC-MSDOS.
mumps	Specifies the EtherType DEC-MUMPS.

Variable	Value
netbios	Specifies the EtherType DEC-Network Basic Input/Output System (NETBIOS).
vines-echo	Specifies the EtherType Virtual Integrated Network Service (VINES) Echo from Banyan systems.
vines-ip	Specifies the EtherType VINES IP.
xns-id	Specifies the EtherType Xerox Network Systems (XNS) protocol suite identifier.
encaptype	Specifies the encapsulation type.
vlan	Specifies the VLAN ID to be filtered.
priority	Specifies the priority of the L2 filter, which is used to decide the applicable rule when the packet matches more than one filter rule. Higher value of filter priority implies a higher priority.
single-tag	Specifies the filter to be applied on single VLAN tagged packets. This parameter is specific to metro package.
double-tag	Specifies the filter to be applied on double VLAN tagged packets. This parameter is specific to metro package.

Defaults

vlan-id	0
priority	1

Related commands

mac access-group

mac access-list extended

deny

show access-lists

Use this command to display the access list configuration.

Command mode

Privileged or user EXEC

Syntax

```
show access-lists
```

Related commands

deny

mac access-group

mac access-list extended

permit

VOIP commands

VoIP subsystem is the analog to Digital Converter (Voice to Data), so that they can be sent as IP packets. VoIP chip is internally connected to BSG.

All FXO and FXS port related configurations and few general configurations of VoIP chip can be done from BSG.

VOIP commands navigation

- reboot voip (page 731)
- set country code (page 732)
- set default codec type (page 733)
- set default g723 encoding rate (page 734)
- set default silent suppression (page 735)
- set digital dial timeout (page 736)
- set dtmf relay (page 737)
- set dtmf rtp payload (page 738)
- set fxo emergency-number (page 739)
- set fxo forward phone-no (page 740)
- set fxo hook detect time (page 741)
- set fxo channel-number (page 742)
- set fxo ring count (page 744)
- set fxs call-forward (page 745)
- set fxs call-forward number (page 746)
- set fxs codec status (page 747)
- set fxs codec type (page 748)
- set fxs display-name (page 749)
- set fxs fax-option (page 750)
- set fxs line (page 751)
- set fxs mailbox number (page 752)
- set fxs mailbox password (page 753)
- set fxs ring type (page 754)
- set fxs user-number (page 755)
- set fxs user-password (page 756)
- set gmt-offset (page 757)
- set ip tos (page 758)
- set ip tos precedence option (page 759)
- set mailbox ip (page 760)
- set pstn-gateway (page 761)
- set voice mailbox (page 762)

- show voip codec config (page 763)
- show voip config (page 764)
- show voip firmware version (page 765)
- show voip status (page 766)
- shutdown (page 767)
- voip1000 (page 768)

reboot voip

Use this command to send the reboot message to VoIP subsystems.

Command mode

VOIP configuration

Syntax

```
reboot voip
```

set country code

Use this command to set the country code for the telephone call progress and error indication tones such as dial tone, busy tone and so on.

Command mode

VOIP Configuration

Syntax

```
set country code { us | uk | japan | china | india | germany |
south-africa | korea | brazil | australia }
```

Variable definitions

This table describes the variables used in the `set country code` command.

Variable	Value
us	Specifies the US Country code.
uk	Specifies the UK Country code.
japan	Specifies the Japan Country code.
china	Specifies the China Country code.
india	Specifies the India Country code.
germany	Specifies the Germany Country code.
south-africa	Specifies the South-Africa Country code.
korea	Specifies the Korea Country code.
brazil	Specifies the Brazil Country code.
australia	Specifies the Australia Country code.

Defaults

us

Related commands

show voip config

set default codec type

Use this command to set the default codec type, preference and frame size.

Command mode

VOIP configuration

Syntax

```
set default codec type {g711u | g711a | g723 | g726 | g729} preference
<integer(1-5 )>frame size <integer(10-120)> milliseconds
```

Variable definitions

This table describes the variables used in the `set default codec type` command.

Variable	Value
codec type	Specifies the codec type. Options: • g711u • g711a • g723 • g726 • g729
preference	Specifies the preferences. The range is from 1 to 5.
frame size	Specifies the frame size. The range is from 10 to 120 milliseconds.

set default g723 encoding rate

Use this command to set the g723 default encoding rate.

Command mode

VOIP configuration

Syntax

```
set default g723 encoding rate {e5dot3|e6dot3}
```

Variable definitions

This table describes the variables used in the `set default g723 encoding rate` command.

Variable	Value
e5dot3	Specifies the e5dot3 encoding rate.
e6dot3	Specifies the e6dot3 encoding rate.

Defaults

e5dot3

set default silent suppression

Use this command to enable or disable default silence suppression.

Command mode

VOIP configuration

Syntax

```
set default {g723|g729} silence suppression {enable|disable}
```

Variable definitions

This table describes the variables used in the `set default {g723|g729} silence suppression` command.

Variable	Value
g723	Specifies the g723 encoding.
g729	Specifies the g729 encoding.
enable|disable	Enables / disables suppression.

Defaults

disable

set digital dial timeout

Use this command to set the digital dial timeout value.

Command mode

VOIP configuration

Syntax

```
set digit dial timeout <integer(500-10000)>
```

Variable definitions

This table describes the variables used in the `set digit dial timeout` command.

Variable	Value
integer (500-10000)	Specifies the timeout in milliseconds for dialing a phone number from FXS lines when # is not pressed. The range is 500 to 10000.

Defaults

5000

set dtmf relay

Use this command to set the DTMF relay option. That is, it sets the options for relaying the DTMF digits during a call.

Command mode

VoIP configuration

Syntax

```
set dtmf relay {rtp | info | none}
```

Variable definitions

This table describes the variables used in the `set dtmf relay` command.

Variable	Value
rtp	Specifies the real time transport protocol.
info	Specifies the information.
none	Specifies no relay option.

Defaults

none

set dtmf rtp payload

Use this command to set the RTP payload type.

Command mode

VoIP configuration

Syntax

```
set dtmf rtp payload <integer(96-127)
```

Variable definitions

This table describes the variables used in the `set dtmf rtp payload` command.

Variable	Value
integer (96-127)	Specifies the RTP dynamic payload type used for relaying DTMF digits over RTP. The range is 96 to 127.

Defaults

101

set fxo emergency-number

Use this command to set the FXO emergency number for contact.

Command mode

FXO Configuration

Syntax

```
set fxo emergency-number < number(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxo emergency-number` command.

Variable	Value
number	Specifies the FXO emergency number.

Defaults

911

Related commands

show voip config

set fxo forward phone-no

Use this command to set the FXO forwarding phone number.

Command mode

FXO Configuration

Syntax

```
set fxo forward phone-no < phone number(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxo forward phone-no` command.

Variable	Value
phone number	Specifies the phone number for which incoming calls to the FXO lines are forwarded.

Defaults

1001

Related commands

show voip config

set fxo hook detect time

Use this command to set the OnHook Detection time of the FXO Channel.

Command mode

FXO Configuration

Syntax

```
set fxo hook detect time <integer(100-10000)> milliseconds
```

Variable definitions

This table describes the variables used in the `set fxo hook detect time` command.

Variable	Value
integer (100-10000)	Specifies the duration in milliseconds for which the FXO line needs to be kept on hook for the PSTN exchange to recognise an hook event. This varies from exchange to exchange. The range is from 100 to 10000 in milliseconds.

Defaults

2000

set fxo channel-number

Use this command to set the Foreign Exchange Office (FXO) channel number.

Command mode

FXO Configuration

Syntax

```
set fxo channel-number <channel(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxo channel-number` command.

Variable	Value
channel	Specifies the FXO channel number.

Defaults

1003

Related commands

show voip config

set fxo phone-number

Use this command to set the Foreign Exchange Office (FXO) phone number.

Command mode

FXO Configuration

Syntax

```
set fxo phone-number <phone number(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxo phone-number` command.

Variable	Value
phone number	Specifies the SIP user ID (phone Number) used for SIP signaling for incoming calls to the FXO line.

Defaults

1003

Related commands

show voip config

set fxo ring count

Use this command to set the FXO maximum number for ring.

Command mode

FXO Configuration

Syntax

```
set fxo ring count < maximum number ring(1-6)>
```

Variable definitions

This table describes the variables used in the `set fxo ring count` command.

Variable	Value
maximum number ring	Specifies the maximum number of rings the FXO line waits before going off Hook.

Defaults

2

Related commands

show voip config

set fxs call-forward

Use this command to enable or disable the call forward on different condition.

Command mode

FXS Configuration

Syntax

```
set fxs call-forward  {on-busy|on-no-answer|unconditional}
{enable|disable}
```

Variable definitions

This table describes the variables used in the `set fxs call-forward` command.

Variable	Value
on-busy	Call Forwarding on busy.
on-no-answer	Call Forwarding on no answer.
unconditional	Call Forwarding unconditional.

set fxs call-forward number

Use this command to set the call forward number.

Command mode

FXS Configuration

Syntax

```
set fxs call-forward number <string(31)>
```

Variable definitions

This table describes the variables used in the `set fxs call-forward number` command.

Variable	Value
string(31)	Specifies the call forward number.

Defaults

0

set fxs codec status

Use this command to set the channel based codec status.

Command mode

FXS Configuration

Syntax

```
set fxs codec status {enable | disable}>
```

Variable definitions

This table describes the variables used in the `set fxs codec status` command.

Variable	Value
enable	Enables channel based codec.
disable	Disables channel based codec.

Defaults

disable

set fxs codec type

Use this command to set the FXS codec type, preference, and frame size.

Command mode

FXS Configuration

Syntax

```
set fxs codec type {g711u | g711a | g723 | g726 | g729} preference
<integer (1-5)> frame size <integer(10-120)> milliseconds
```

Variable definitions

This table describes the variables used in the `set fxs codec type` command.

Variable	Value
codec type	Specifies the codec type. Options: • g711u • g711a • g723 • g726 • g729
preference	Specifies the preference. The range is from 1to 5.
frame size	Specifies the frame size. The range is from 10 to 120 milliseconds.

set fxs display-name

Use this command to set the FXS display Name.

Command mode

FXS Configuration

Syntax

```
set fxs display-name < name(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxs display-name` command.

Variable	Value
name	Specifies the SIP display name.

Defaults

Unknown

Related commands

show voip config

set fxs fax-option

Use this command to set the fax option for FXS.

Command mode

FXS Configuration

Syntax

```
set fxs fax-option {disabled|transparent|foip-voice }
```

Variable definitions

This table describes the variables used in the `set fxs fax-option` command.

Variable	Value
disabled	Disables the fax option for FXS.
transparent	Renegotiates SIP for codec change to G711mu. Disables silence suppression and echo canceller.
foip-voice	Renegotiates SIP for T.38 fax over IP gateway.

Defaults

disabled

Related commands

show voip config

set fxs line

Use this command to set the FXS Line Status as enabled or disabled.

Command mode

FXS Configuration

Syntax

```
set fxs line {enable|disable}
```

Variable definitions

This table describes the variables used in the `set fxs line` command.

Variable	Value
enable	Enables the FXS Line status.
disable	Disables the FXS Line status.

Defaults

disabled

Related commands

show voip config

set fxs mailbox number

Use this command to set the FXS mailbox number.

Command mode

FXS Configuration

Syntax

```
set fxs mailbox number <number(31)>
```

Variable definitions

This table describes the variables used in the `set fxs mailbox number` command.

Variable	Value
number (31)	Specifies the voicemail box number at the voicemail server.

Defaults

0

set fxs mailbox password

Use this command to set the FXS mailbox password.

Command mode

FXS Configuration

Syntax

```
set fxs mailbox password <string(31)>
```

Variable definitions

This table describes the variables used in the `set fxs mailbox password` command.

Variable	Value
string (31)	Specifies the voicemail authentication password.

Defaults

0

set fxs ring type

Use this command to set the FXS ring type.

Command mode

FXS Configuration

Syntax

```
set fxs ring type <integer(0-2)>
```

Variable definitions

This table describes the variables used in the `set fxs ring type` command.

Variable	Value
integer (0-2)	Specifies the ring type. The range is from 0 to 2 in milliseconds.

Defaults

0

set fxs user-number

Use this command to set the FXS user number.

Command mode

FXS Configuration

Syntax

```
set fxs user-number < number(length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxs user-number` command.

Variable	Value
number	Specifies the SIP user ID.

Defaults

1001 (line 1)

1002 (line 2)

Related commands

show voip config

set fxs user-password

Use this command to set the FXS password for the user.

Command mode

FXS Configuration

Syntax

```
set fxs user-password <password (length<=31)>
```

Variable definitions

This table describes the variables used in the `set fxs user-password` command.

Variable	Value
password	Specifies the SIP authentication password for REGISTER and INVITE.

Defaults

0

Related commands

show voip config

set gmt-offset

Use this command to set the offset from GMT for local time.

Command mode

VOIP Configuration

Syntax

```
set gmt-offset < offset value (integer -12 to +12)>
```

Variable definitions

This table describes the variables used in the `set gmt-offset` command.

Variable	Value
offset value	Specifies the GMT offset value for time zone calculation. Range is from -12 to +12.

Defaults

0

Related commands

show voip config

set ip tos

Use this command to enable or disable the IP TOS.

Command mode

VOIP configuration

Syntax

```
set ip tos {delay | throughput | reliability} {enable | disable}
```

Variable definitions

This table describes the variables used in the `set ip tos` command.

Variable	Value
delay	Specifies the IP TOS delay.
throughput	Specifies the IP TOS throughput.
reliability	Specifies the IP TOS reliability.

set ip tos precedence option

Use this command to set the IP TOS precedence option.

Command mode

VOIP configuration

Syntax

```
set ip tos precedence option <integer(0-7)>
```

Variable definitions

This table describes the variables used in the `set digit dial timeout` command.

Variable	Value
integer (0-7)	Specifies the IP TOS preference setting for RTP and SIP packets. The range is from 0 to 7.

Defaults

0

set mailbox ip

Use this command to set the voice mail server Ip address and server port.

Command mode

VOIP configuration

Syntax

```
set mailbox ip <ucast_addr> port <integer(1024-65535)>
```

Variable definitions

This table describes the variables used in the `set mailbox ip` command.

Variable	Value
ucast_addr	Specifies the voice mail server Hostname or IP Address.
integer (1024-65535)	Specifies the voice mail server port number. The range is from 1 to 65535

Defaults

ucast_addr	0.0.0.0
port	5060

set pstn-gateway

Use this command to set the Public Switched Telephone Network (PSTN) line status.

Command mode

FXO Configuration

Syntax

```
set pstn-gateway {enable|disable}
```

Variable definitions

This table describes the variables used in the `set pstn-gateway` command.

Variable	Value
enable	Enables the FXO line.
disable	Disables the FXO line.

Defaults

disabled

Related commands

show voip config

set voice mailbox

Use this command to enable or disable the voice mail status.

Command mode

VOIP configuration

Syntax

```
set voice mailbox {enable|disable}
```

Variable definitions

This table describes the variables used in the `set voice mailbox` command.

Variable	Value
enable	Enables the voice mail status.
disable	Disables the voice mail status.

Defaults

disable

show voip codec config

Use this command to display the FXS and the Global Codec configuration.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show voip {global | fxs} codec config
```

Variable definitions

This table describes the variables used in the `show voip codec config` command.

Variable	Value
global	Specifies the Global codec configuration.
fxs	Specifies the FXS codec configuration.

show voip config

Use this command to display the configurations of VoIP.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show voip {global | fxo | fxs} config
```

Variable definitions

This table describes the variables used in the `show voip config` command.

Variable	Value
global	Specifies the Global codec configuration.
fxo	Specifies the FXO Configuration.
fxs	Specifies the FXS codec configuration.

Related Commands

set fxs user-number

set fxo ring count

set fxo ring count

set fxs user-number

set fxs display-name

set fxs user-password

set fxs fax-option

set gmt-offset

reboot voip

show voip firmware version

Use this command to display the firmware version.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show voip firmwareversion
```

show voip status

Use this command to display the firmware version.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show voip status
```

shutdown

Use this command to shutdown the admin status of the VoIP module. You can configure the FXO, FXS, and VoIP only when the admin status is shutdown.

Command mode

VoIP1000 configuration

Syntax

```
shutdown


no shutdown
```

voip1000

Use this command to enter the VOIP configuration mode.

Command mode

Global Configuration

Syntax

```
voip1000
```

Technical Report 069 commands

Use Technical Report (TR) 069 commands to configure TR 069. TR 069 is a DSL Forum technical specification entitled *CPE WAN Management Protocol* (CWMP). This specification defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, the forum provides the communication between the CPE and the Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

TR 069 commands navigation

- acs url (page 770)
- connection request (page 771)
- periodic inform (page 772)
- periodic inform interval (page 773)
- send inform (page 774)
- show mgmt server config (page 775)
- show tr69 status (page 776)
- tr69 (page 777)

acs url

Use this command to configure the HTTP or HTTPS URL, user name and password of the ACS.

Command mode

TR 069

Syntax

```
acs url <http|https> user <username> passwd <password>
```

Variable definitions

This table describes the variables used in the `acs url` command.

Variable	Value
http|https	Specifies the URL, which starts with http:// or https://.
user name	Specifies the user name for the Management Server. It is a random string.
password	Specifies the password for the user name.

Related Commands

show mgmt server config (page 775)

connection request

Use this command to add the user name and password for CPE URL.

Command mode

TR 069

Syntax

```
connection request url user <username> passwd <password>
```

Variable definitions

This table describes the variables used in the `connection request` command.

Variable	Value
user name	Specifies the user name for the Management Server.
password	Specifies the password for the user name.

Related Commands

show mgmt server config

periodic inform

Use this command to enable or disable the periodic inform interval.

Command mode

TR 069

Syntax

```
periodic inform {enable | disable}
```

Variable definitions

This table describes the variables used in the `periodic inform` command.

Variable	Value
enable	Enables the periodic inform interval.
disable	Disables the periodic inform interval.

Related Commands

show mgmt server config

periodic inform interval

Use this command to configure the periodic inform interval in seconds.

Command mode

TR 069

Syntax

```
periodic inform interval <integer(35-4294967295)secs>
```

Variable definitions

This table describes the variables used in the `periodic inform interval` command.

Variable	Value
interger	Specifies the periodic inform interval value in seconds.

Defaults

60 seconds

Related Commands

show mgmt server config

send inform

Use this command to send an inform forcibly to the ACS.

Command mode

TR 069

Syntax

```
send inform
```

Related Commands

acs url

show mgmt server config

Use this command to display the CPE Management Server configuration.

Command mode

Privileged or User EXEC

Syntax

```
show mgmt server config
```

show tr69 status

Use this command to display the CPE status.

Command mode

Privileged or User EXEC

Syntax

```
show tr69 status
```

tr69

Use this command to enter the tr69 mode.

Command mode

Tr-69

Syntax

```
tr69
```

Wireless commands

This section describes the commands that helps you to configure the wireless command line interface (CLI).

Wireless commands navigation

- Wireless local area network commands (page 780)
- Digital Subscriber Line commands (page 821)
- T1/E1 commands (page 831)

Wireless local area network commands

The Wireless Local Area Network (WLAN) module controls the configuration of the wireless access point (AP) connected to the Business Service Gateway (BSG). It configures the radio parameters and Service Set Identifier (SSID) based parameters in the AP. The authentication mode, WiFi Protected Access (WPA) mode, and pass phrases are configured in the AP using this module. This module also provides the front end for getting station- and radio-based statistics from the wireless AP.

WLAN commands navigation

- config ap country (page 782)
- config dot11—network (page 783)
- config dot11 beaconperiod (page 784)
- config dot11 channel (page 785)
- config dot11 dtim (page 786)
- config dot11 fragmentation (page 787)
- config dot11 mode (page 788)
- config dot11 preamble (page 789)
- config dot11 profile clients (page 790)
- config dot11 protection (page 791)
- config dot11 rts-threshold (page 792)
- config dot11 supported rates (page 793)
- config dot11 turbo (page 794)
- config dot11 txpower (page 795)
- config dot11 wmm (page 796)
- config dot11 wmm-acknowledge-policy (page 797)
- config dot11 wmmparam (page 798)
- config macfilter (page 799)
- config wlan (page 800)
- config wlan broadcast-ssid (page 801)
- config wlan create (page 802)
- config wlan delete (page 803)
- config wlan interface (page 804)
- config wlan mac-filtering (page 805)
- config wlan pmksa timeout (page 806)
- config wlan security cipher-suite (page 808)
- config wlan security preauth (page 809)
- config wlan security pre-shared-key (page 810)
- config wlan security static-wep-key encryption (page 811)
- config wlan wep default-key (page 812)

- debug wlan (page 813)
- no wlan static-wep-key encryption (page 814)
- show AP status (page 815)
- show client ap global (page 816)
- show dot11 (page 817)
- show mac-filter-info (page 818)
- show wep default-key-info (page 819)
- show wlan (page 820)

config ap country

Use this command to set the country code.

Command mode

Global configuration

Syntax

```
config ap country <country string>
```

Variable definitions

This table describes the variables used in the `config ap country` command.

Variable	Value
country string	Enter country code.

config dot11—network

Use this command to enable or disable the radios.

Command mode

Radio configuration

Syntax

```
config dot11 {enable | disable} network
```

Variable definitions

This table describes the variables used in the `config dot11` command.

Variable	Value
enable | disable	Enable or disable the radios.

Related commands

`show dot11`

config dot11 beaconperiod

Use this command to configure the beaconperiod for radios.

Command mode

Radio configuration

Syntax

```
config dot11 beaconperiod <beaconperiod(20-1000)>
```

Related commands

show dot11

config dot11 channel

Use this command to set the radio channel.

Command mode

Radio configuration

Syntax

```
config dot11 channel { auto | <channel value (1-11)> }
```

Variable definitions

This table describes the variables used in the `config dot11 channel` command.

Variable	Value
auto	Automatically detect the radio-channel.
channel value	Manual radio channel configuration. The value ranges from 1 to 11.

Related commands

`show dot11`

config dot11 dtim

Use this command to configure the DTIM period for radios.

Command mode

Radio configuration

Syntax

```
config dot11 dtim <DTIM Period(1-255)>
```

Related commands

show dot11

config dot11 fragmentation

Use this command to configure the fragmentation threshold for radios.

Command mode

Radio configuration

Syntax

```
config dot11 fragmentation <Fragmentation Threshold(256-2356)>
```

Related commands

show dot11

config dot11 mode

Use this command to set the radio mode.

Command mode

Radio configuration

Syntax

```
config dot11 mode {b | g | bg}
```

Variable definitions

This table describes the variables used in the `config dot11 mode` command.

Variable	Value
b | g | bg	Mode of operation for radios of type bg.

Related commands

`show dot11`

config dot11 preamble

Use this command to set the preamble parameter.

Command mode

Radio configuration

Syntax

```
config dot11 preamble <short|short-or-long>
```

Variable definitions

This table describes the variables used in the `config dot11 preamble` command.

Variable	Value
short	Short preamble.
short-or-long	Short or long preamble.

Related commands

`show dot11`

config dot11 profile clients

Use this command to set the maximum clients.

Command mode

Radio configuration

Syntax

```
config dot11 profile clients <integer(0-63)>
```

Variable definitions

This table describes the variables used in the `config dot11 profile` command.

Variable	Value
integer	Specifies the maximum number of profile clients. Range is from 0 to 64.

Related commands

`show dot11`

config dot11 protection

Use this command to set the protection method.

Command mode

Radio configuration

Syntax

```
config dot11 protection {cts-only | rts-cts | none}
```

Variable definitions

This table describes the variables used in the `config dot11 protection` command.

Variable	Value
cts-only	Specifies the cts-only protection method.
rts-cts	Specifies the rts-cts protection method.
none	Specifies no protection method.

Related commands

`show dot11`

config dot11 rts-threshold

Use this command to set the rts-threshold of the radios.

Command mode

Radio configuration

Syntax

```
config dot11 rts-threshold <threshold value(0-2347)>
```

Related commands

show dot11

config dot11 supported rates

Use this command to set the supported wireless speed.

Command mode

Radio configuration

Syntax

```
config dot11 supported rates <values (1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps)>
```

Variable definitions

This table describes the variables used in the `config dot11 supported rates` command.

Variable	Value
`values (1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps)`	Specifies the wireless speed values in Mbps.

Related commands

`show dot11`

config dot11 turbo

Use this command to set the turbo mode.

Command mode

Radio configuration

Syntax

```
config dot11 turbo {static|dynamic|disable}
```

Variable definitions

This table describes the variables used in the `config dot11 turbo` command.

Variable	Value
static	Specifies the static turbo mode.
dynamic	Specifies the dynamic turbo mode.
disable	Specifies that there are no wireless clients that support turbo mode.

Related commands

`show dot11`

config dot11 txpower

Use this command to set the power levels.

Command mode

Radio configuration

Syntax

```
config dot11 txpower { minimum | eigth | quarter | half | full }
```

Variable definitions

This table describes the variables used in the `config dot11 txpower` command.

Variable	Value
auto	Automatically detects the power level.
powerlevel	Specifies the Tx Power levels. Range is from 0 to 17.

Related commands

`show dot11`

config dot11 wmm

Use this command to set the status of Wireless MultiMedia (WMM).

Command mode

Radio configuration

Syntax

```
config dot11 wmm {disabled | supported | required}
```

Variable definitions

This table describes the variables used in the `config dot11 wmm` command.

Variable	Value
disabled | supported | required	Specifies the WMM status.

Related commands

`show dot11`

config dot11 wmm-acknowledge-policy

Use this command to set the acknowledge policy for each number.

Command mode

Radio configuration

Syntax

```
config dot11 wmm-acknowledge-policy <ac number(1-4)> {ack | noack}
```

Variable definitions

This table describes the variables used in the `config dot11 wmm-acknowledge-policy` command.

Variable	Value
ac number	Specifies the access categories. Range is from 1 to 4.
ack | noack	Specifies acknowledgement or no acknowledgement.

Related commands

`show dot11`

config dot11 wmmparam

Use this command to set the WMM parameters.

Command mode

Radio configuration

Syntax

```
config dot11 wmmparam <ac number(1-4)> <LogAcCwMin(1-15)>
<LogAcCwMax(1-15)> <AcAIFS(1-15)> <AcTxOpLimit(0-65535)>
<BssLogCwMin(1-15)> <BssLogCwMax(1-15)> <BssAIFS(1-15)>
<BssTxOpLimit(0-65535)>
```

Variable definitions

This table describes the variables used in the `config dot11 wmmparam` command.

Variable	Value
ac number	Specifies the access categories. Value ranges from 1 to 4.
LogAcCwMin	Specifies the minimum contention width. Value ranges from 1 to 15.
LogAcCwMax	Specifies maximum contention width. Value ranges from 1 to 15.
AcAIFS	Specifies the arbitrary interframe sequence. Values ranges from 0 to 15.
AcTxOpLimit	Specifies the transmission opportunity. Value ranges from 0 to 65535.
ssLogCwMin	Specifies the minimum contention width. Value ranges from 1 to 15.
BssLogCwMax	Specifies maximum contention width. Value ranges from 1 to 15.
BssAIFS	Specifies the arbitration interframe space. Values ranges from 0 to 8192.
BssTxOpLimit	Specifies the transmit opportunity. Value ranges from 0 to 15.

Related commands

`show dot11`

config macfilter

Use this command to add or delete the MAC filter table entry.

Command mode

Global configuration

Syntax

```
config macfilter {add | del} <Mac Address> [{allow | deny}]
```

Variable definitions

This table describes the variables used in the `config macfilter` command.

Variable	Value
add | del	Add or delete the mac filter table entry.
Mac Address	Specifies the station MAC address.
allow | deny	Allow or deny the station.

Related commands

`show mac-filter-info`

config wlan

Use this command to enable or disable WLAN.

Command mode

Global configuration

Syntax

```
config wlan { enable | disable } <Wlan-Id(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan` command.

Variable	Value
enable | disable	Enable or disable WLAN.
Wlan-Id	WLAN identifier. Range is from 1 to 4.

Related commands

`config wlan create`

`show wlan`

config wlan broadcast-ssid

Use this command to configure broadcast SSID status.

Command mode

Global configuration

Syntax

```
config wlan broadcast-ssid { enable | disable } <Wlan-Id(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan broadcast-ssid` command.

Variable	Value
enable | disable	Enable or disable SSID broadcast.
Wlan-Id	WLAN identifier. Value ranges from 1 to 4.

Defaults

config wlan broadcast-ssid	enable

Related commands

`show wlan`

config wlan create

Use this command to create a BSG with WLAN ID and Service Set Identifier (SSID).

Command mode

Global configuration

Syntax

```
Config wlan create <wlanid(1-4)> <ssid>
```

Variable definitions

This table describes the variables used in the `config wlan create` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. The value ranges from 1 to 4.
ssid	Specifies the SSID. The length of string or number is 1 to 32.

Related commands

`config wlan delete`

`show wlan`

config wlan delete

Use this command to delete a BSG for the specified WLAN ID.

Command mode

Global configuration

Syntax

```
Config wlan delete <wlan-id(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan delete` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.

Related commands

`config wlan create`

`show wlan`

config wlan interface

Use this command to configure the VLAN ID for the specified WLAN ID.

Command mode

Global configuration

Syntax

```
config wlan interface <Wlan-id(1-4)> <vlan-interface-name>
```

Variable definitions

This table describes the variables used in the `config wlan interface` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.
vlan-interface-name	Specifies the VLAN interface name.

Defaults

vlan-interface-name	vlan1

Related commands

`show wlan`

config wlan mac-filtering

Use this command to configure the WLAN MAC filtering.

Command mode

Global configuration

Syntax

```
config wlan mac-filtering {allow | deny}
```

Variable definitions

This table describes the variables used in the `config wlan mac-filtering` command.

Variable	Value
allow	Allows MAC addresses that are not configured.
deny	Denies MAC addresses that are not configured.

Defaults

Mac filtering is set to allow by default.

Related commands

`show mac-filter-info`

config wlan pmksa timeout

Use this command to the Pairwise Master Key Security Association (PMKSA) timeout value.

Command mode

Global configuration

Syntax

```
config wlan pmksa timeout <Wlan-Id(1-4)> <timeout value(60-604800)>
```

Variable definitions

This table describes the variables used in the `config wlan pmksa timeout` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Range is 1 to 4.
timeout value	Specifies the PMKSA timeout value. Value ranges from 60 to 604800.

Related commands

`show wlan`

config wlan security auth-type

Use this command to set the authentication type.

Command mode

Global configuration

Syntax

```
config wlan security auth-type { open | shared | wpa | wpa2 |
wpa-wpa2-mixed | wpa-psk | wpa2-psk | wpa-wpa2-psk-mixed | open1x }
<wlan-Id(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan security auth-type` command.

Variable	Value
open | shared	Specifies the authentication mode (open or shared).
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.

Related commands

`show wlan`

config wlan security cipher-suite

Use this command to configure the encryption cipher suite.

Command mode

Global configuration

Syntax

```
config wlan security cipher-suite {aes-ccmp | tkip | wep | aes-ccmp-tkip
| aes-ccmp-tkip | tkip-wep | aes-ccmp-tkip-wep} <integer(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan security cipher-suite` command.

Variable	Value
aes-ccmp | tkip | wep | aes-ccmp-tkip | aes-ccmp-tkip | tkip-wep | aes-ccmp-tkip-wep	Specifies the encryption types.
integer	Specifies the WLAN identifier. Value ranges from 1 to 4.

Related commands

`show wlan`

config wlan security preauth

Use this command to enable or disable 802.11i preauthentication.

Command mode

Global configuration

Syntax

```
config wlan security preauth { enable | disable } <Wlan-id(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan security preauth` command.

Variable	Value
enable | disable	Enables or disables 802.11i pre-authentication.
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.

Defaults

config wlan security preauth	enable

Related commands

`show wlan`

config wlan security pre-shared-key

Use this command to provide options to enter the PSK.

Command mode

Global configuration

Syntax

```
config wlan security pre-shared-key <Wlan-Id(1-4)> {hex | ascii} <key>
```

Variable definitions

This table describes the variables used in the `config wlan security pre-shared-key` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.
{hex | ascii} <key>	Specifies the value for the key. Value can be: hexadecimal (0-9, A-F) of maximum length 64. ASCII, or any printable characters whose length can be in the range of 8 to 63.

Related commands

`show wlan`

config wlan security static-wep-key encryption

Use this command to configure static WEP keys and indexes.

Command mode

Global configuration

Syntax

```
config wlan security static-wep-key encryption <wlanId(1-4)>
{64|128|152} {hex | ascii} <key> <keyIndex(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan security static-wep-key encryption` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.
64|128|152	Specifies the value of the key length.
{hex | ascii} <key>	Specifies the value as hexadecimal, 0-9, A-F, ASCII or any printable characters.
keyIndex	Specifies the wep key index. Value ranges from 1 to 4.

Related commands

`show wep default-key-info`

config wlan wep default-key

Use this command to configure the WEP default key index of the particular SSID.

Command mode

Global configuration

Syntax

```
config wlan wep default-key <Wlan-Id(1-4)> <key-index(1-4)>
```

Variable definitions

This table describes the variables used in the `config wlan wep default-key` command.

Variable	Value
Wlan-Id	Specifies the WLAN identifier. Value ranges from 1 to 4.
key-Index	Specifies the wep key index. Value ranges from 1 to 4.

Related commands

`show wlan`

debug wlan

Use this command to display current trace or add new trace. Precede this command with no to remove the trace.

Command mode

Privileged EXEC

Syntax

```
debug wlan [all] [rpc] [fn-entry] [fn-exit] [critical] [fail] [debug]
[wd]


no debug wlan [all] [rpc] [fn-entry] [fn-exit] [critical] [fail] [debug]
[wd]
```

Variable definitions

This table describes the variables used in the `debug wlan` command.

Variable	Value
all	Specifies all traces.
rpc	Specifies RPC related traces.
critical	Specifies critical related traces.
fn-entry	Specifies the function entry related traces.
fn-exit	Specifies the function exit related traces.
fail	Specifies the failure related traces.
debug	Specifies the debug related traces.
wd	Specifies the wd related traces.

Defaults

Debugging is disabled

no wlan static-wep-key encryption

Use this command to remove the static WEP keys. Precede this command with no to remove the trace.

Command mode

Global configuration

Syntax

```
no wlan static-wep-key encryption <wlanId(1-4)> <keyIndex(1-4)>
```

Variable definitions

This table describes the variables used in the `no wlan static-wep-key encryption` command.

Variable	Value
wlanId	Specifies the WLAN ID. Value ranges from 1 to 4.
keyIndex	Specifies the key index. Value ranges from 1 to 4.

Related commands

```
show wep default-key-info
```

show AP status

Use this command to display the AP Status.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show ap status
```

show client ap global

Use this command to display information about stations.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show client ap global
```

show dot11

Use this command to display all or specific 802.11 configurations.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dot11 [<radio arbitrary index>]
```

Related commands

config dot11 beaconperiod

config dot11 channel

config dot11 dtim

config dot11 fragmentation

config dot11 mode

config dot11–network

config dot11 preamble

config dot11 supported rates

config dot11 wmm-acknowledge-policy

config dot11 wmmparam

show mac-filter-info

Use this command to display the MAC filter table.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show mac-filter-info
```

Related commands

`config macfilter`

`config wlan mac-filtering`

show wep default-key-info

Use this command to display WEP default key table per SSID.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show wep default-key-info <Wlan-Id>
```

Variable definitions

This table describes the variables used in the `show wep default-key-info` command.

Variable	Value
Wlan-Id	Specifies the WLAN ID.

Related commands

`config wlan security static-wep-key encryption`

show wlan

Use this command to display the information of all or a particular BSG.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show wlan [<Wlan-Id>]
```

Variable definitions

This table describes the variables used in the `show wlan` command.

Variable	Value
Wlan-Id	Specifies the WLAN ID.

Related commands

`config wlan`

`config wlan broadcast-ssid`

`config wlan create`

`config wlan delete`

`config wlan interface`

`config wlan interface`

`config wlan security preauth`

`config wlan security pre-shared-key`

`config wlan security static-wep-key encryption`

`config wlan wep default-key`

Digital Subscriber Line commands

The Digital Subscriber Line (DSL) module controls the configuration and control of the DSL modem connected to the CAS. It is responsible for configuring the ATM parameters of the modem. This module also provides the front end for getting the statistics of the DSL modem. These commands are executed only on BSG 12 platforms.

DSL navigation

- dsl operating-mode (page 822)
- encapsulation (page 823)
- traffic parameters set (page 828)
- show dsl interface (page 825)
- show dsl interface pvc (page 826)
- show dsl traffic (page 827)
- traffic parameters set (page 828)
- qos set (page 824)
- vci value (page 830)

dsl operating-mode

Use this command to set the operating mode of the DSL modem.

Command mode

DSL interface configuration

Syntax

```
dsl operating-mode { auto | t1413 | gdmt | glite | adsl2 | adsl2plus }
```

Variable definitions

This table describes the variables used in the `dsl operating-mode` command.

Variable	Value
auto	Specifies the auto DSL operating mode. The operation mode will be negotiated with the DSLAM.
t1413	Specifies the t1413 DSL operating mode. Operates at 8 Mbps Downstream speed and 1Mbps Upstream speed.
gdmt	Specifies the gdmt DSL operating mode. Operates at 8 Mbps Downstream speed and 1Mbps Upstream speed.
glite	Specifies the glite DSL operating mode. Operates at 1.5 Mbps Downstream speed and 0.5Mbps Upstream speed.
adsl2	Specifies the adsl2 DSL operating mode. Operates at 12 Mbps Downstream speed and 1Mbps Upstream speed.
adsl2plus	Specifies the adsl2plus DSL operating mode. Operates at 24 Mbit/s Downstream rate and 1Mbit/s Upstream rate.

Defaults

auto

Related commands

`show dsl traffic`

encapsulation

Use this command to set the protocol encapsulation.

Command mode

PVC interface configuration

Syntax

```
encapsulation { aa15snap | vcmux }
```

Variable definitions

This table describes the variables used in the `encapsulation` command.

Variable	Value
aa15snap	Specifies the ATM Adaptation Layer 5/Sub Network Access Protocol.
vcmux	Specifies the virtual channel multiplexer.

Defaults

aa15snap

Related commands

`show dsl interface`

`show dsl interface pvc`

qos set

Use this command to set the QOS parameters for the DSL modem. (CBR = 0, VBR = 1, or UBR = 2).

Command mode

PVC interface configuration

Syntax

```
qos set <qos_val>
```

Variable definitions

This table describes the variables used in the `qos set` command.

Variable	Value
qos_val	Specifies the QOS value. Range is 0 to 2.

Related commands

`show dsl interface`

`show dsl interface pvc`

show dsl interface

Use this command to displays the DSL interface configuration.

Command mode

Privileged EXEC/User EXEC Mode

Syntax

```
show dsl interface
```

Related commands

`qos set`

`vci value`

`traffic parameters set`

`traffic parameters set`

`encapsulation`

show dsl interface pvc

Use this command to configure PVC.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dsl interface pvc <ifnum>
```

Variable definitions

This table describes the variables used in `show dsl interface pvc` command.

Variable	Value
ifnum	Specifies DSL/PVC Interface Identifier. Example is 1/1.

Related commands

`qos set`

`vci value`

`traffic parameters set`

`traffic parameters set`

`encapsulation`

show dsl traffic

Use this command to display the DSL Statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show dsl traffic
```

Related Command

`dsl operating-mode`

traffic parameters set

Use this command to set the traffic parameters of the DSL modem.

Command mode

PVC interface configuration

Syntax

```
traffic parameters set <pcr> <scr> <mbs>
```

Variable definitions

This table describes the variables used in the `traffic parameters set` command.

Variable	Value
pcr	Specifies the peak cell rate (PCR). Value ranges from 0 to 65535.
scr	Specifies the sustainable cell rate. Value ranges from 0 to 65535.
mbs	Specifies the maximum burst size. Value ranges from 0 to 65535.

Defaults

pcr	4000
scr	4000
mbs	10

Related commands

`show dsl interface`

`show dsl interface pvc`

vpi value

Use this command to configure the Virtual Path Identifier (VPI) value. The VPI and Virtual Channel Identifier (VCI) numbers are the connection parameters required for the DSL Modem to connect to the DSL Provider.

Command mode

PVC interface configuration

Syntax

```
vpi <vpbi value>
```

Variable definitions

This table describes the variables used in the `vpi value` command.

Variable	Value
vpi value720	Specifies Virtual Path Identifier value. Range is 0 to 255.

Defaults

vpi

Related commands

`show dsl interface`

`show dsl interface pvc`

vci value

Use this command to configure the Virtual Channel Identifier (VCI) value.

Command mode

PVC interface configuration

Syntax

```
vci <vci value>
```

Variable definitions

This table describes the variables used in the `vci value` command.

Variable	Value
vci value	Specifies the VCI value. Value ranges from 0 to 255.

Defaults

vci

Related commands

`show dsl interface`

`show dsl interface pvc`

T1/E1 commands

T1/E1 is a digital WAN carrier facility. T1 transmits DS-1 formatted data at 1.544 Mbps and E1 transmits E1 formatted data at 2.048 Mbps through the telephone switch network using HDB3, AMI, or B8Zs coding. This commands are executed only on the BSG12 platforms.

T1/E1 commands navigation

- cablelength long (page 832)
- cablelength short (page 833)
- channel-group (page 834)
- clear controller (page 835)
- clear controller statistics table (page 836)
- clock source (page 837)
- controller (page 838)
- controller mode (page 839)
- debug t1e1 (page 840)
- dump t1e1 sib-counter (page 841)
- framing (page 842)
- linecode (page 843)
- line status change trap (page 844)
- loopback (page 845)
- mode (page 846)
- sendcode (page 847)
- show controllers (page 848)
- show controller statistics interval (page 849)
- show controller statistics table (page 850)
- show controllers t1e1 channel-groups (page 851)

cablelength long

Use this command to set the Line Build Out of the T1 to various values. Precede the command with `no` to restore the default line configuration to Short Haul(DSU). This command is for the BSG12 platform.

Command mode

T1/E1 configuration

Syntax

```
cablelength long { neg225db | neg15db | neg75db | zerodb }


no cablelength long
```

Variable definitions

This table describes the variables used in the `cablelength long` command.

Variable	Value
neg225db	Specifies the cable length value of neg225db.
neg15db	Specifies the cable length value of neg15db.
neg75db	Specifies the cable length value of neg75db.
zerodb	Specifies the cable length value of zerodb.

cablelength short

Use this command to set the Line Length for the T1-DSU line. This command is for the BSG12 platform.

Command mode

T1/E1 configuration

Syntax

```
cablelength short {133 | 266 | 399 | 533 | 655}
```

Variable definitions

This table describes the variables used in the `cablelength short` command.

Variable	Value
133	Specifies the cable length of 133.
266	Specifies the cable length of 266.
399	Specifies the cable length of `399`.
533	Specifies the cable length of 533.
655	Specifies the cable length of 655.

channel-group

Use this command to define the time slots that belongs to each group on the T1 or E1 circuit. Precede this command with `no` to delete the channel group from the T1/E1 link. The maximum number of channel groups that can be created is 16. This command is for the BSG12 platform.

Command mode

T1/E1 configuration

Syntax

```
channel-group <group-id> timeslots <range>
no channel-group <group-id>
```

Variable definitions

This table describes the variables used in the `channel-group` command.

Variable	Value
group-id	Specifies the group identifier.
range	Specifies the range of time slots. • T1—The values ranges from 1 to 24. • E1—The values ranges from 2 to 32.

clear controller

Use this command to reset the T1 or E1 controller to default mode (T1). This command deletes all HDLC interfaces created. On execution of this command the specified T1/E1 controller is set to its default configuration and all the HDLC interfaces created on the controller are unstacked and deleted from the PPP interfaces. This command is only for the BSG12 platform.

Command mode

Global configuration

Syntax

```
clear controller { t1 | e1 } <T1E1Index>
```

Variable definitions

This table describes the variables used in the `clear controller` command.

Variable	Value
T1E1Index	T1/E1 link identifier.

clear controller statistics table

Use this command to clear the statistics table for the T1/E1 link.

Command mode

T1/E1 configuration

Syntax

```
clear controller statistics table {{current | interval | total} {local |
remote} | all} [<integer(1-10)>]
```

Variable definitions

This table describes the variables used in the `clear controller statistics table` command.

Variable	Value
current	Specifies the current statistics table.
interval	Specifies the interval statistics table.
total	Specifies the total statistics table.
local	specifies the near end statistics.
remote	Specifies the remote statistics.
all	Specifies all statistics.
integer (1-10)	Specifies T1/E1 link identifier.

clock source

Use this command to select the clock source for the Time Division Multiplexing (TDM). Precede this command with no to configure the clock source to its default string.

Command mode

T1/E1 configuration

Syntax

```
clock source {local | remote | throughTiming}


no clock source
```

Variable definitions

This table describes the variables used in `clock source` command.

Variable	Value
local	Specifies the local clock source.
remote	Specifies the remote clock source.
throughTiming	Specifies the through timing clock source. Takes the adjacent T1/E1 link clock source.

controller

Use this command to configure a T1 or E1 controller and enter T1/E1 controller configuration mode.

Command mode

Global configuration

Syntax

```
controller {t1 | e1} <T1E1Index>
```

Variable definitions

This table describes the variables used in `controller` command.

Variable	Value
t1	Specifies the T1 type controller.
e1	Specifies E1 type controller.
T1E1Index	Specifies the T1/E1 link identifier. The value ranges from dependent on the number of T1/E1 links.

Defaults

controller	t1

controller mode

Use this command to configure a T1 or E1 controller as T1 or E1 mode.

Command mode

Global configuration

Syntax

```
controller mode { t1 | e1 }
```

Variable definitions

This table describes the variables used in `controller mode` command.

Variable	Value
t1	Specifies the T1 mode.
e1	Specifies the E1 mode.

Defaults

t1

debug t1e1

Use this command to enable debug option for the T1/E1 module. Precede this command with `no` to disable the debug options for the T1/E1 module.

Command mode

Privileged EXEC

Syntax

```
debug t1e1 {[failure] [resource] [timer] | [all]}


no debug t1e1 {[failure] [resource] [timer] | [all]}
```

Variable definitions

This table describes the variables used in `debug t1e1` command.

Variable	Value
failure	Failure traces.
resource	Resource traces.
timer	Timer related traces.
all	All traces.

Defaults

Debugging is disabled

dump t1e1 sib-counter

Use this command to display the LLP SIB counter statistics.

Command mode

Privileged EXEC or User EXEC

Syntax

```
dump t1e1 sib-counter
```

framing

Use this command to select the frame type for the T1 or E1 data line.

Command mode

T1/E1 configuration

Syntax

```
framing {esf | sf | e1 | e1-crc4}
```

Variable definitions

This table describes the variables used in the `framing` command.

Variable	Value
esf	Specifies extended super frame type.
sf	Specifies super frame type.
e1	Specifies the basic E1 type.
e1-crc4	Specifies E1 with CRC4 type.

Related commands

`show controllers`

linecode

Use this command to select the line code type for the T1 or E1 line.

Command mode

T1/E1 configuration

Syntax

```
linecode {b8zs | hdb3 | ami}
```

Variable definitions

This table describes the variables used in the `linecode` command.

Variable	Value
b8zs	Specifies B8ZS line code type.
hdb3	Specifies HDB3 line code type.
ami	Specifies Alternate Mark Invention (AMI) line code type.

Related commands

`show controllers`

line status change trap

Use this command to set the trap state for the line status change for the T1/E1 link.

Command mode

T1/E1 configuration

Syntax

```
line status change trap {enable | disable}
```

Variable definitions

This table describes the variables used in the `Line Status Change Trap` command.

Variable	Value
enable	Enables trap state for line status change for the T1/E1 link.
disable	Disables trap state for line status change for the T1/E1 link.

loopback

Use this command to loop an entire T1/E1 line (including all channel groups defined on the controller) towards loop back mode. Precede this command with no to remove the T1/E1 loop back mode.

Command mode

T1/E1 configuration

Syntax

```
loopback {local | remote-liu | remote-framer | dual}


no loopback
```

Variable definitions

This table describes the variables used in the `loopback` command.

Variable	Value
local	Specifies local loopback mode.
remote-framer	Specifies remote loopback framer mode.
dual	Specifies dual loopback mode.
remote-liu	Specifies remote loopback LIU mode.

mode

Use this command to set the T1 Line Mode to either CSU (Long Haul) or DSU (Short Haul).

Command mode

T1/E1 configuration

Syntax

```
mode { csu | dsu }
```

Variable definitions

This table describes the variables used in the `mode` command.

Variable	Value
csu	Specifies channel service units.
dsu	Specifies data service units.

sendcode

Use this command to select the data pattern to send on the T1/E1 line. Precede the command with `no` to disable the test data pattern.

Command mode

T1/E1 configuration

Syntax

```
sendcode {SendQRS | Pattern511}


no sendcode
```

Variable definitions

This table describes the variables used in the `sendcode` command.

Variable	Value
SendQRS	Specifies the SendQRS data pattern.
Pattern511	Specifies the Pattern511 data pattern.

show controllers

Use this command to display T1/E1 controller configurations for the T1/E1 link.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show controllers {t1 | e1} [T1E1Index]
```

Variable definitions

This table describes the variables used in the `show controller` command.

Variable	Value
t1	Specifies the T1 controller configurations for T1 link.
e1	Specifies the E1 controller configurations for E1 link.
T1E1Index	Specifies the T1/E1 link identifier.

Related commands

`framing`

`linecode`

`loopback`

show controller statistics interval

Use this command to display T1/E1 interval statistics for the T1/E1 link.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show controller statistics interval <interval> <T1E1Index>
```

Variable definitions

This table describes the variables used in the `show controller statistics interval` command.

Variable	Value
interval	Specifies the interval statistics range.
T1E1Index	Specifies the T1/E1 link identifier.

show controller statistics table

Use this command to display the T1/E1 current or total table statistics for the local-end or remote-end T1/E1 link.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show controllers statistics table {  current | total | all }  [T1E1Index]
```

Variable definitions

This table describes the variables used in the `show controller statistics table` command.

Variable	Value
current	Specifies the current statistics for T1/E1 link.
total	Specifies the total table statistics for the T1/E1 link.
all	Specifies both the current and total table statistics for the T1/E1 link.
T1E1Index	Specifies the T1/E1 link identifier.

show controllers t1e1 channel-groups

Use this command to display the channel groups present on the T1E1 controller.

Command mode

Privileged EXEC or User EXEC

Syntax

```
show controllers t1e1 channel-groups]
```

vendorid

Use this command to set the T1/E1 hardware transmission vendors circuit identifier.

Command mode

T1/E1 configuration

Syntax

```
vendorid <T1E1 hardware vendor>
```

Variable definitions

This table describes the variables used in the `vendorid` command.

Variable	Value
T1E1 hardware vendor	Specifies the T1/E1 hardware vendor string.

Appendix A - Target based commands

This section describes all the target based commands. The commands described in this section can be run on any target but not on a linux environment.

Target based commands navigation

- negotiation (page 854)
- speed (page 855)
- duplex (page 856)
- mac-address-table aging-time (page 857)
- databits (page 858)
- parity (page 859)
- speed - console (page 860)
- stopbits (page 861)

negotiation

Use this command to enable the auto-negotiation on the interface. Precede this command with `no` to disable the auto-negotiation on the interface.

Command mode

Interface configuration

Syntax

```
negotiation
no negotiation
```

speed

Use this command to set the speed of the interface. Precede this command with `no` to set the speed of the interface to its default value.

Command mode

Interface configuration

Syntax

```
speed { 10 | 100 | 1000 | 10000 | auto }


no speed
```

Variable definitions

This table describes the variables used in the `speed` command.

Variable	Value
10	Specifies the speed of the port as 10 Mbps.
100	Specifies the speed of the port as 100 Mbps.
1000	Specifies the speed of the port as 1000 Mbps.
10000	Specifies the speed of the port as 10000 Mbps.
auto	Port automatically detects the speed it must run on based on the peer switch.

Defaults

auto

Related commands

negotiation

duplex

duplex

Use this command to configure the duplex operation. Precede this command with `no` to configure the duplex operation to the default value.

Command mode

Interface configuration

Syntax

```
duplex { full | half }


no duplex
```

Variable definitions

This table describes the variables used in the `duplex` command.

Variable	Value
full	Specifies that port is in full-duplex mode.
half	Specifies that port is in half-duplex mode.

Defaults

full

Related commands

negotiation

speed

mac-address-table aging-time

Use this command to set the maximum age of a dynamically learnt entry in the MAC address table. Precede this command with `no` to set the maximum age of an entry in the MAC address table to its default value.

Command mode

Global configuration

Syntax

```
mac-address-table aging-time <10-1000000 seconds>


no mac-address-table aging-time
```

Defaults

300

databits

Use this command to specify the number of databits per character for this console. Precede this command with `no` to reset the console databits to the default setting.

Command mode

Line configuration

Syntax

```
databits <number (5-8)>


no databits
```

Variable definitions

This table describes the variables used in the `databits` command.

Variable	Value
number (5-8)	Specifies the number of databits per character. Range is from 5 to 8.

Defaults

8

Related commands

parity

speed

parity

Use this command to set the parity for the console connection. Precede this command with `no` to reset the console parity to the default setting.

Command mode

Line configuration

Syntax

```
parity {even | odd | none}


no parity
```

Variable definitions

This table describes the variables used in the `parity` command.

Variable	Value
even	Specifies the even parity.
odd	Specifies the odd parity.
none	Specifies no parity.

Defaults

none

Related commands

databits

speed

speed - console

Use this command to set the transmit and receive speeds for the serial console. Precede this command with `no` to reset the baud rate to the default setting.

Command mode

Line configuration

Syntax

```
speed <baud-rate (50-460800)>


no speed
```

Variable definitions

This table describes the variables used in the `speed` command.

Variable	Value
baud-rate	Specifies the baud rate (Bits per second) of the connection. Range is from 50 to 460800.

Defaults

9600

Related commands

databits

parity

stopbits

Use this command to set the number of stopbits for the console connection. Precede this command with `no` to reset the default settings.

Command mode

Line configuration

Syntax

```
stopbits {1 | 2}
```

```
no stopbits
```

Variable definitions

This table describes the variables used in the `stopbits {1 | 2}` command.

Variable	Value
1	Specifies one stopbit.
2	Specifies two stopbits.

Defaults

1

Related commands

speed

databits

parity