Cisco 500 Series Stackable Managed Switches, Release 1.3.7
# Table of Contents

1. **Summary of New/Modified Features for 500 Family, Release 1.3.7**  .... 25  
2. **Introduction** ........................................................................................ 26  
3. **User Interface Commands** ................................................................. 47  
   - enable ........................................................................................................ 47  
   - disable ....................................................................................................... 48  
   - login .......................................................................................................... 48  
   - configure ................................................................................................. 49  
   - exit (Configuration) .................................................................................. 50  
   - exit (EXEC) ............................................................................................. 50  
   - end ............................................................................................................ 51  
   - help .......................................................................................................... 52  
   - history ....................................................................................................... 53  
   - history size ............................................................................................... 54  
   - terminal history ....................................................................................... 55  
   - terminal history size ................................................................................ 55  
   - terminal datadump .................................................................................... 56  
   - terminal width .......................................................................................... 57  
   - terminal prompt ....................................................................................... 58  
   - show history ............................................................................................. 59  
   - show privilege ......................................................................................... 60  
   - do .............................................................................................................. 60  
   - banner exec .............................................................................................. 61  
   - banner login ............................................................................................. 63  
   - show banner .............................................................................................. 65  
4. **Macro Commands** .............................................................................. 66  
   - macro name ............................................................................................... 66  
   - macro ........................................................................................................ 69  
   - macro description ..................................................................................... 71  
   - macro global .............................................................................................. 73  
   - macro global description .......................................................................... 75  
   - show parser macro .................................................................................... 76  
5. **RSA and Certificate Commands** ....................................................... 79  
   - crypto key generate dsa .......................................................................... 80  
   - crypto key generate rsa .......................................................................... 81  
   - crypto key import ..................................................................................... 82  
   - show crypto key ....................................................................................... 84  
   - crypto certificate generate ...................................................................... 85  
   - crypto certificate request ........................................................................ 87  
   - crypto certificate import .......................................................................... 89  
   - show crypto certificate ........................................................................... 95
6 System Management Commands ................................................................. 98
  ping ................................................................. 98
  traceroute ............................................................ 101
  telnet ............................................................... 104
  resume .............................................................. 107
  hostname ......................................................... 108
  reload ............................................................. 109
  show reload ..................................................... 111
  service cpu-utilization ........................................ 112
  show cpu utilization .......................................... 112
  show users ..................................................... 113
  show sessions ................................................ 114
  show system .................................................. 115
  show environment ......................................... 116
  show inventory ............................................... 119
  show version ................................................ 120
  show version md5 ............................................ 121
  set system ..................................................... 121
  show system mode ......................................... 124
  show system languages ................................... 125
  show system tcam utilization ............................ 126
  show services tcp-udp ...................................... 126
  show tech-support .......................................... 127
  system recovery ............................................ 129
  show system fans .......................................... 129
  show system sensors ..................................... 130
  show system id .............................................. 132
  disable ports leds ......................................... 133
  show ports leds configuration .......................... 133

7 SSH Client Commands ............................................................................. 135
  ip ssh-client authentication ................................ 135
  ip ssh-client change server password ................... 136
  ip ssh-client key ............................................. 137
  ip ssh-client password .................................... 140
  ip ssh-client server authentication ..................... 141
  ip ssh-client server fingerprint ......................... 142
  ip ssh-client source-interface .......................... 143
  ipv6 ssh-client source-interface ......................... 144
  ip ssh-client username .................................... 145
  show ip ssh-client .......................................... 146
  show ip ssh-client server ................................ 149

8 Stack Commands .................................................................................. 152
  stack master .................................................... 152
  stack standalone .............................................. 153
  stack native .................................................... 153
write memory ................................................................. 219
write ................................................................. 220
delete ................................................................. 220
dir ................................................................. 221
more ................................................................. 223
rename ................................................................. 224
boot system ............................................................... 225
show bootvar .............................................................. 226
show running-config ....................................................... 227
show startup-config ....................................................... 230
service mirror-configuration ........................................... 232
show mirror-configuration service ................................... 234

12 Auto-Configuration ........................................................................ 235
boot host auto-config .......................................................... 235
show boot ................................................................. 236
ip dhcp tftp-server ip address ............................................ 237
ip dhcp tftp-server file ...................................................... 238
show ip dhcp tftp-server ..................................................... 238

13 Management ACL Commands ....................................................... 240
management access-list ..................................................... 240
permit (Management) ......................................................... 241
deny (Management) .......................................................... 242
management access-class ................................................... 244
show management access-list ............................................ 244
show management access-class ......................................... 245

14 Network Management Protocol (SNMP) Commands ......................... 247
snmp-server server ............................................................ 247
snmp-server community ..................................................... 247
snmp-server community-group ............................................. 249
snmp-server source-interface .............................................. 250
snmp-server source-interface-ipv6 ..................................... 252
snmp-server view .............................................................. 253
show snmp views .............................................................. 254
snmp-server group ............................................................ 255
show snmp groups ............................................................. 257
snmp-server user .............................................................. 258
show snmp users .............................................................. 260
snmp-server filter ............................................................. 263
show snmp filters ............................................................. 264
snmp-server host .............................................................. 265
snmp-server engineID local ............................................... 267
snmp-server engineID remote ............................................. 268
show snmp engineID ........................................................ 269
snmp-server enable traps ................................................... 270
snmp-server trap authentication ......................................... 270
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Web Server Commands</td>
<td>277</td>
</tr>
<tr>
<td></td>
<td>ip http server</td>
<td>277</td>
</tr>
<tr>
<td></td>
<td>ip http port</td>
<td>277</td>
</tr>
<tr>
<td></td>
<td>ip http timeout-policy</td>
<td>278</td>
</tr>
<tr>
<td></td>
<td>ip http secure-server</td>
<td>279</td>
</tr>
<tr>
<td></td>
<td>ip https certificate</td>
<td>280</td>
</tr>
<tr>
<td></td>
<td>show ip http</td>
<td>280</td>
</tr>
<tr>
<td></td>
<td>show ip https</td>
<td>281</td>
</tr>
<tr>
<td>16</td>
<td>Telnet, Secure Shell (SSH) and Secure Login (Slogin) Commands</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>ip telnet server</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>ip ssh server</td>
<td>284</td>
</tr>
<tr>
<td></td>
<td>ip ssh port</td>
<td>284</td>
</tr>
<tr>
<td></td>
<td>ip ssh password-auth</td>
<td>285</td>
</tr>
<tr>
<td></td>
<td>ip ssh pubkey-auth</td>
<td>286</td>
</tr>
<tr>
<td></td>
<td>crypto key pubkey-chain ssh</td>
<td>287</td>
</tr>
<tr>
<td></td>
<td>user-key</td>
<td>288</td>
</tr>
<tr>
<td></td>
<td>key-string</td>
<td>289</td>
</tr>
<tr>
<td></td>
<td>show ip ssh</td>
<td>291</td>
</tr>
<tr>
<td></td>
<td>show crypto key pubkey-chain ssh</td>
<td>292</td>
</tr>
<tr>
<td>17</td>
<td>Line Commands</td>
<td>294</td>
</tr>
<tr>
<td></td>
<td>line</td>
<td>294</td>
</tr>
<tr>
<td></td>
<td>speed</td>
<td>294</td>
</tr>
<tr>
<td></td>
<td>autobaud</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>exec-timeout</td>
<td>296</td>
</tr>
<tr>
<td></td>
<td>show line</td>
<td>297</td>
</tr>
<tr>
<td>18</td>
<td>Bonjour Commands</td>
<td>299</td>
</tr>
<tr>
<td></td>
<td>bonjour enable</td>
<td>299</td>
</tr>
<tr>
<td></td>
<td>bonjour interface range</td>
<td>299</td>
</tr>
<tr>
<td></td>
<td>show bonjour</td>
<td>300</td>
</tr>
<tr>
<td>19</td>
<td>Authentication, Authorization and Accounting (AAA) Commands</td>
<td>302</td>
</tr>
<tr>
<td></td>
<td>aaa authentication login</td>
<td>302</td>
</tr>
<tr>
<td></td>
<td>aaa authentication enable</td>
<td>303</td>
</tr>
<tr>
<td></td>
<td>login authentication</td>
<td>305</td>
</tr>
<tr>
<td></td>
<td>enable authentication</td>
<td>306</td>
</tr>
<tr>
<td></td>
<td>ip http authentication</td>
<td>307</td>
</tr>
<tr>
<td></td>
<td>show authentication methods</td>
<td>309</td>
</tr>
<tr>
<td></td>
<td>password</td>
<td>310</td>
</tr>
<tr>
<td></td>
<td>enable password</td>
<td>310</td>
</tr>
</tbody>
</table>
20 RADIUS Commands ................................................................. 326
   radius-server host ......................................................... 326
   radius-server key .......................................................... 328
   radius-server retransmit ............................................... 329
   radius-server host source-interface .............................. 329
   radius-server host source-interface-ipv6 ........................ 330
   radius-server timeout .................................................. 331
   radius-server deadtime ............................................... 332
   show radius-servers .................................................... 333
   show radius-servers key ............................................... 334

21 TACACS+ Commands ............................................................. 335
   tacacs-server host ...................................................... 335
   tacacs-server key ........................................................ 336
   tacacs-server timeout .................................................. 337
   tacacs-server host source-interface .............................. 338
   tacacs-server host source-interface-ipv6 ........................ 339
   show tacacs ............................................................... 340
   show tacacs key .......................................................... 341

22 SYSLOG Commands ............................................................. 342
   logging on ................................................................. 342
   logging host .............................................................. 343
   logging source-interface .............................................. 344
   logging source-interface-ipv6 ....................................... 345
   logging console ........................................................... 346
   logging buffered .......................................................... 346
   clear logging ............................................................... 348
   logging file ................................................................. 348
   clear logging file ........................................................ 349
   aaa logging ................................................................. 350
   file-system logging ..................................................... 351
   logging aggregation on ................................................ 351
   logging aggregation aging-time .................................... 352
   logging origin-id .......................................................... 353
   show logging ............................................................... 354
   show logging file ........................................................ 355
23 Remote Network Monitoring (RMON) Commands ........................................... 358

show rmon statistics ................................................................. 358
rmon collection stats ............................................................. 360
show rmon collection stats ....................................................... 361
show rmon history ................................................................. 362
rmon alarm .............................................................................. 364
show rmon alarm-table ........................................................... 366
show rmon alarm ................................................................. 367
rmon event ............................................................................. 369
show rmon events ................................................................. 370
show rmon log ...................................................................... 371
rmon table-size ................................................................. 372

24 802.1X Commands ........................................................................... 374

aaa authentication dot1x .......................................................... 374
clear dot1x statistics ............................................................... 375
data ..................................................................................... 376
dot1x auth-not-req ................................................................. 377
dot1x authentication ............................................................... 378
dot1x guest-vlan ................................................................. 379
dot1x guest-vlan enable .......................................................... 380
dot1x guest-vlan timeout ......................................................... 381
dot1x host-mode ................................................................. 382
dot1x max-hosts ................................................................. 385
dot1x max-login-attempts ....................................................... 386
dot1x max-req ................................................................. 387
dot1x page customization ......................................................... 388
dot1x port-control ................................................................. 389
dot1x radius-attributes vlan .................................................. 390
dot1x re-authenticate ............................................................. 392
dot1x reauthentication .......................................................... 393
dot1x system-auth-control ...................................................... 393
dot1x timeout quiet-period ..................................................... 394
dot1x timeout reauth-period ................................................... 395
dot1x timeout server-timeout .................................................. 396
dot1x timeout silence-period .................................................. 397
dot1x timeout supp-timeout .................................................... 398
dot1x timeout tx-period ......................................................... 399
dot1x traps authentication failure .......................................... 400
dot1x traps authentication quiet .............................................. 401
dot1x traps authentication success ........................................ 402
dot1x unlock client ............................................................... 403
dot1x violation-mode ............................................................ 404
show dot1x ................................................................. 405
show dot1x locked clients ....................................................... 410
25 Ethernet Configuration Commands .............................................................. 414
  interface ................................................................. 414
  interface range ................................................... 415
  shutdown ............................................................. 416
  operation time ..................................................... 417
  description ......................................................... 418
  speed ................................................................. 419
  duplex ................................................................. 420
  negotiation .......................................................... 421
  flowcontrol .......................................................... 422
  mdix ................................................................. 423
  back-pressure ...................................................... 424
  port jumbo-frame ................................................ 424
  clear counters ..................................................... 425
  set interface active ............................................... 426
  errdisable recovery cause ...................................... 426
  errdisable recovery interval ................................... 427
  errdisable recovery reset ....................................... 428
  show interfaces configuration .................................. 429
  show interfaces status .......................................... 430
  show interfaces advertise ....................................... 431
  show interfaces description .................................... 433
  show interfaces counters ....................................... 434
  show ports jumbo-frame ......................................... 437
  show errdisable recovery ....................................... 438
  show errdisable interfaces ...................................... 438
  storm-control broadcast enable ............................... 439
  storm-control broadcast level ................................ 440
  storm-control include-multicast ............................. 441
  show storm-control ............................................... 442

26 PHY Diagnostics Commands ................................................................. 443
  test cable-diagnostics tdr ....................................... 443
  show cable-diagnostics tdr ..................................... 444
  show cable-diagnostics cable-length ......................... 445
  show fiber-ports optical-transceiver ......................... 446

27 Power over Ethernet (PoE) Commands ....................................................... 448
  power inline .......................................................... 448
  power inline inrush test disable .............................. 449
  power inline legacy support disable ......................... 449
  power inline powered-device ................................... 450
  power inline priority ............................................. 451
  power inline usage-threshold .................................. 451
  power inline traps enable ...................................... 452
spanning-tree bpduguard ................................................................. 537
spanning-tree bpdu (Interface) ......................................................... 536
spanning-tree pathcost method ....................................................... 534
spanning-tree link-type ................................................................. 533
spanning-tree priority ................................................................. 529
spanning-tree disable ................................................................. 530
spanning-tree cost ................................................................. 530
spanning-tree port-priority ............................................................ 531
spanning-tree portfast ................................................................. 532
spanning-tree link-type ................................................................. 533
spanning-tree pathcost method ....................................................... 534
spanning-tree bpdu (Global) .......................................................... 535
spanning-tree bpdu (Interface) ......................................................... 536
spanning-tree guard root ............................................................... 537
spanning-tree bpduguard ................................................................. 537
clear spanning-tree detected-protocols ........................................... 538
spanning-tree mst priority ............................................................. 539
spanning-tree mst max-hops ......................................................... 540
spanning-tree mst port-priority ....................................................... 541
spanning-tree mst cost ................................................................. 542
spanning-tree mst configuration ..................................................... 543
instance (MST) ........................................................................ 543
name (MST) ........................................................................... 544
revision (MST) ......................................................................... 545
show (MST) ............................................................................... 546
exit (MST) ................................................................................ 547
abort (MST) ........................................................................... 547
show spanning-tree .................................................................. 548

32 Port Monitor Commands .................................................................. 522
port monitor ............................................................................... 522
show ports monitor ................................................................... 524

33 Spanning-Tree Commands ................................................................ 525
34 Virtual Local Area Network (VLAN) Commands .............................................................. 561

- vlan database .................................................................................................................. 561
- vlan .................................................................................................................................. 562
- show vlan .......................................................................................................................... 562
- default-vlan vlan .............................................................................................................. 564
- show default-vlan-membership ......................................................................................... 565
- interface vlan .................................................................................................................... 566
- interface range vlan ......................................................................................................... 567
- name .................................................................................................................................. 568
- switchport protected-port ............................................................................................... 569
- show interfaces protected-ports ...................................................................................... 570
- switchport mode ............................................................................................................... 571
- switchport access vlan ..................................................................................................... 572
- switchport trunk allowed vlan ......................................................................................... 573
- switchport trunk native vlan ............................................................................................ 574
- switchport general allowed vlan ..................................................................................... 576
- switchport general pvid ..................................................................................................... 577
- switchport general ingress-filtering disable ...................................................................... 579
- switchport general acceptable-frame-type ....................................................................... 580
- switchport customer vlan ............................................................................................... 581
- map protocol protocols-group .......................................................................................... 582
- switchport general map protocols-group vlan ................................................................. 583
- show vlan protocols-groups ............................................................................................ 584
- map mac macs-group ........................................................................................................ 585
- switchport general map macs-group vlan ........................................................................ 586
- show vlan macs-groups .................................................................................................... 587
- switchport forbidden default-vlan .................................................................................... 588
- switchport forbidden vlan ............................................................................................... 589
- switchport default-vlan tagged ....................................................................................... 590
- show interfaces switchport .............................................................................................. 592
- switchport access multicast-tv vlan ................................................................................ 594
- switchport customer multicast-tv vlan ............................................................................. 595
- show vlan multicast-tv ...................................................................................................... 596
- ip internal-usage-vlan ...................................................................................................... 597
- show vlan internal usage .................................................................................................. 598
- vlan prohibit-internal-usage ............................................................................................. 599

35 Voice VLAN Commands ................................................................................................ 602

- voice vlan state ............................................................................................................... 602
- voice vlan refresh ............................................................................................................. 605
- voice vlan id ..................................................................................................................... 606
- voice vlan vpt .................................................................................................................. 607
- voice vlan dscp ............................................................................................................... 608
- voice vlan oui-table ........................................................................................................ 609
- voice vlan cos mode ....................................................................................................... 611
36 SSD Commands ................................................................. 621
   ssd config ................................................................. 621
   passphrase ................................................................. 621
   ssd rule ................................................................. 622
   show SSD ................................................................. 625
   ssd session read ....................................................... 626
   show ssd session ....................................................... 627
   ssd file passphrase control ...................................... 628
   ssd file integrity control .......................................... 629

37 Smartport Commands .................................................. 631
   macro auto (Global) .................................................. 631
   macro auto smartport (Interface) ................................ 632
   macro auto trunk refresh ......................................... 633
   macro auto resume .................................................. 634
   macro auto persistent .............................................. 635
   macro auto smartport type ....................................... 636
   macro auto processing cdp ...................................... 638
   macro auto processing lldp ....................................... 639
   macro auto processing type ..................................... 640
   macro auto user smartport macro ............................ 641
   macro auto built-in parameters ............................... 642
   show macro auto processing ..................................... 643
   show macro auto smart-macros .................................. 644
   show macro auto ports ............................................ 646
   smartport switchport trunk allowed vlan .................. 648
   smartport switchport trunk native vlan ..................... 649
   smartport storm-control broadcast enable .................. 649
   smartport storm-control broadcast level ................... 650
   smartport storm-control include-multicast ............... 651

38 CDP Commands .......................................................... 653
   cdp run ................................................................. 653
   cdp enable ............................................................ 654
   cdp pdu ................................................................. 654
   cdp advertise-v2 ..................................................... 655
   cdp appliance-tlv enable ........................................... 656
   cdp mandatory-tlvs validation ................................... 657
   cdp source-interface ............................................... 658
   cdp log mismatch duplex ......................................... 659
   cdp log mismatch voip .............................................. 659
   cdp log mismatch native .......................................... 660
39 Link Layer Discovery Protocol (LLDP) Commands ................................................. 679

lldp run ................................................................. 679
lldp transmit ......................................................... 679
lldp receive .......................................................... 680
lldp timer ............................................................... 681
lldp hold-multiplier .................................................. 682
lldp reinit ............................................................... 683
lldp tx-delay ........................................................... 683
lldp optional-tlv ..................................................... 684
lldp optional-tlv 802.1 .............................................. 685
lldp management-address .......................................... 686
lldp notifications ................................................... 688
lldp notifications interval ......................................... 688
lldp lldpdu ............................................................ 689
lldp med ................................................................. 690
lldp med notifications topology-change ......................... 691
lldp med fast-start repeat-count .................................. 692
lldp med network-policy (global) .................................. 693
lldp med network-policy (interface) ............................... 694
lldp med network-policy voice auto ............................... 695
clear lldp table ....................................................... 696
lldp med location ..................................................... 697
lldp chassis-id ......................................................... 698
show lldp configuration ........................................... 699
show lldp med configuration ...................................... 701
show lldp local tlv 802.1 ............................................. 703
show lldp local ........................................................ 704
show lldp neighbors ................................................. 706
show lldp statistics .................................................. 712

40 IGMP Snooping Commands ............................................................................. 716

ip igmp snooping (Global) ........................................... 716
ip igmp snooping vlan ............................................... 716
ip igmp snooping vlan mrourter ................................... 717
ip igmp snooping vlan mrourter interface .......................... 718
41 IPv6 MLD Snooping Commands ................................................................. 736

- ip igmp snooping vlan forbidden mrouter .................................................. 719
- ip igmp snooping vlan static ................................................................. 720
- ip igmp snooping map cpe vlan .............................................................. 722
- ip igmp snooping query address .............................................................. 723
- ip igmp snooping vlan querier ................................................................. 724
- ip igmp snooping vlan querier address ..................................................... 724
- ip igmp snooping vlan querier version ...................................................... 725
- ip igmp robustness .................................................................................. 726
- ip igmp query-interval ............................................................................. 727
- ip igmp query-max-response-time ............................................................. 728
- ip igmp last-member-query-count ............................................................ 728
- ip igmp last-member-query-interval .......................................................... 729
- ip igmp snooping vlan immediate-leave .................................................... 730
- show ip igmp snooping mrouter ............................................................... 731
- show ip igmp snooping interface .............................................................. 731
- show ip igmp snooping groups ................................................................. 733
- show ip igmp snooping multicast-tv .......................................................... 734
- show ip igmp snooping cpe vlans ............................................................. 735

42 Link Aggregation Control Protocol (LACP) Commands ............................... 750

- lacp system-priority .................................................................................. 750
- lacp port-priority ...................................................................................... 750
- lacp timeout ............................................................................................ 751
- show lacp ................................................................................................. 752
- show lacp port-channel ............................................................................. 754

43 GARP VLAN Registration Protocol (GVRP) Commands ............................... 756

- gvrp enable (Global) ................................................................................. 756
- gvrp enable (Interface) .............................................................................. 756
- gvrp vlan-creation-forbid ........................................................................... 757
44 DHCP Snooping and ARP Inspection Commands ................................................. 763
  ip dhcp snooping ................................................................. 763
  ip dhcp snooping vlan ......................................................... 764
  ip dhcp snooping trust ....................................................... 764
  ip dhcp snooping information option allowed-untrusted ............... 765
  ip dhcp snooping verify ...................................................... 766
  ip dhcp snooping database .................................................. 767
  ip dhcp snooping database update-freq .................................. 767
  ip dhcp snooping binding .................................................... 768
  clear ip dhcp snooping database .......................................... 769
  show ip dhcp snooping ....................................................... 770
  show ip dhcp snooping binding ............................................ 771
  ip source-guard .............................................................. 772
  ip source-guard binding ................................................... 773
  ip source-guard tcam retries-freq ...................................... 774
  ip source-guard tcam locate ............................................... 775
  show ip source-guard configuration ..................................... 776
  show ip source-guard status .............................................. 777
  show ip source-guard inactive ............................................ 778
  show ip source-guard statistics ......................................... 779
  ip arp inspection ............................................................ 780
  ip arp inspection vlan ..................................................... 781
  ip arp inspection trust ..................................................... 781
  ip arp inspection validate ................................................ 782
  ip arp inspection list create ............................................ 783
  ip mac ............................................................................. 784
  ip arp inspection list assign .............................................. 785
  ip arp inspection logging interval ...................................... 786
  show ip arp inspection ....................................................... 787
  show ip arp inspection list ................................................ 787
  show ip arp inspection statistics ........................................ 788
  clear ip arp inspection statistics ....................................... 789

45 IP Addressing Commands ........................................................................... 790
  ip address ........................................................................... 790
  ip address dhcp .................................................................. 792
  renew dhcp ......................................................................... 793
  ip default-gateway ............................................................ 794
  show ip interface .................................................................. 795
  arp ....................................................................................... 796
  arp timeout (Global) .......................................................... 797
46 IPv6 Router Commands ................................................................. 807

- clear ipv6 neighbors .............................................................. 807
- clear ipv6 prefix-list .............................................................. 807
- ipv6 address .......................................................................... 808
- ipv6 address anycast .............................................................. 809
- ipv6 address autoconfig .......................................................... 811
- ipv6 address eui-64 ................................................................. 812
- ipv6 address link-local ........................................................... 813
- ipv6 default-gateway .............................................................. 815
- ipv6 enable ............................................................................ 815
- ipv6 hop-limit ...................................................................... 816
- ipv6 icmp error-interval .......................................................... 817
- ipv6 link-local default zone ..................................................... 818
- ipv6 mld version .................................................................... 819
- ipv6 nd advertisement-interval ............................................... 820
- ipv6 nd dad attempts .............................................................. 821
- ipv6 nd hop-limit ................................................................... 823
- ipv6 nd managed-config-flag ................................................... 824
- ipv6 nd ns-interval .................................................................. 825
- ipv6 nd other-config-flag ......................................................... 826
- ipv6 nd prefix ....................................................................... 827
- ipv6 nd ra interval .................................................................. 831
- ipv6 nd ra lifetime ................................................................... 832
- ipv6 nd ra suppress ................................................................. 833
- ipv6 nd reachable-time ............................................................ 834
- ipv6 nd router-preference ......................................................... 835
- ipv6 neighbor ....................................................................... 837
- ipv6 prefix-list ..................................................................... 839
- ipv6 redirect ......................................................................... 843
- ipv6 route ............................................................................ 844
- ipv6 unicast-routing ............................................................... 846
- ipv6 unreachables ................................................................. 847
- show ipv6 interface ............................................................... 848
- show ipv6 link-local default zone .......................................... 857
- show ipv6 nd prefix ............................................................... 858
- show ipv6 neighbors ............................................................. 859
- show ipv6 prefix-list ............................................................ 861
47 Tunnel Commands ................................................................. 872
  interface tunnel .............................................................. 872
  tunnel destination .......................................................... 872
  tunnel isatap solicitation-interval ..................................... 873
  tunnel isatap robustness ................................................... 874
  tunnel isatap router ......................................................... 875
  tunnel mode ipv6ip .......................................................... 876
  tunnel source ............................................................... 878
  show ipv6 tunnel ............................................................ 880

48 DHCP Relay Commands ....................................................... 883
  ip dhcp relay enable (Global) ............................................. 883
  ip dhcp relay enable (Interface) ........................................ 883
  ip dhcp relay address (Global) .......................................... 884
  ip dhcp relay address (Interface) ...................................... 885
  show ip dhcp relay .......................................................... 886
  ip dhcp information option ............................................... 889
  show ip dhcp information option ....................................... 889

49 IP Routing Protocol-Independent Commands .......................... 891
  accept-lifetime ............................................................. 891
  ip route ................................................................. 893
  ip routing ................................................................. 895
  key-string ................................................................. 896
  key (key chain) ........................................................... 897
  key chain ................................................................. 899
  send-lifetime .............................................................. 901
  show ip protocols ........................................................ 903
  show ip route ............................................................. 904
  show key chain .......................................................... 907

50 ACL Commands .................................................................. 910
  ip access-list (IP standard) ............................................... 910
  ip access-list (IP extended) ............................................. 911
  permit (IP) ................................................................. 912
  deny (IP) ................................................................. 915
  ipv6 access-list (IPv6 extended) ....................................... 918
  permit (IPv6) ............................................................. 919
  deny (IPv6) ............................................................... 922
  mac access-list ........................................................... 924
  permit (MAC) ............................................................. 925
  deny (MAC) ............................................................... 926
  service-acl input .......................................................... 928
  time-range ................................................................. 929
51  Quality of Service (QoS) Commands................................. 936

absolute ................................................................. 931
periodic ................................................................. 932
show time-range ....................................................... 933
show access-lists ....................................................... 933
show interfaces access-lists ........................................ 935

qos ................................................................. 936
qos advanced-mode trust .......................................... 937
show qos ............................................................... 938
class-map .............................................................. 939
show class-map ......................................................... 940
match ................................................................. 941
policy-map ............................................................. 942
class ................................................................. 943
show policy-map ....................................................... 944
trust ................................................................. 945
set ................................................................. 947
police ................................................................. 948
service-policy ........................................................ 949
qos aggregate-policer ................................................ 950
show qos aggregate-policer ........................................ 952
police aggregate ....................................................... 953
wrr-queue cos-map .................................................... 954
wrr-queue bandwidth ............................................... 955
priority-queue out num-of-queues ................................ 956
traffic-shape ......................................................... 957
traffic-shape queue .................................................. 958
rate-limit (Ethernet) .................................................. 959
rate-limit (VLAN) ..................................................... 960
qos wrr-queue wrtd .................................................. 961
show qos wrr-queue wrtd ............................................ 962
show qos interface ..................................................... 963
qos map policed-dscp .............................................. 967
qos map dscp-queue .................................................. 968
qos trust (Global) ...................................................... 969
qos trust (Interface) ................................................... 971
qos cos ............................................................. 971
qos dscp-mutation ................................................... 972
qos map dscp-mutation .............................................. 973
show qos map ........................................................ 974
clear qos statistics ................................................... 975
qos statistics policer ................................................ 976
qos statistics aggregate-policer ................................... 977
qos statistics queues ................................................ 977
show qos statistics ..................................................... 978
52 Denial of Service (DoS) Commands ................................................................. 980
  security-suite deny syn-fin ................................................................. 980
  security-suite syn protection mode .................................................. 980
  security-suite syn protection threshold ........................................... 982
  security-suite syn protection recovery ............................................ 982
  show security-suite syn protection .................................................... 983
  security-suite enable .................................................................. 984
  security-suite dos protect .............................................................. 986
  security-suite dos syn-attack ........................................................... 987
  security-suite deny martian-addresses ......................................... 988
  security-suite deny syn ................................................................. 990
  security-suite deny icmp ................................................................. 991
  security-suite deny syn-attack ......................................................... 993
  show security-suite configuration ................................................... 994

53 VRRP Commands ............................................................................. 996
  clear vrrp counters ................................................................... 996
  show vrrp .................................................................................. 997
  show vrrp counters ................................................................... 1000
  vrrp description ....................................................................... 1002
  vrrp ip ....................................................................................... 1002
  vrrp preempt ............................................................................. 1004
  vrrp priority ............................................................................. 1005
  vrrp shutdown ........................................................................... 1006
  vrrp source-ip ............................................................................ 1006
  vrrp timers advertise .................................................................. 1007
  vrrp version .............................................................................. 1008

54 RIP Commands .................................................................................. 1010
  clear rip statistics ..................................................................... 1010
  default-information originate ....................................................... 1010
  default-metric ........................................................................... 1012
  ip rip authentication key-chain ..................................................... 1013
  ip rip authentication mode ............................................................ 1014
  ip rip authentication-key ............................................................... 1015
  ip rip default-information originate ........................................... 1016
  ip rip distribute-list in ................................................................. 1016
  ip rip distribute-list out ............................................................... 1017
  ip rip offset ............................................................................... 1018
  ip rip passive-interface ............................................................... 1019
  ip rip shutdown ...................................................................... 1020
  network ..................................................................................... 1021
  passive-interface (RIP) ................................................................. 1022
  redistribute (RIP) .................................................................... 1023
  router rip .................................................................................. 1026
  show ip rip database .................................................................. 1027
  show ip rip peers ...................................................................... 1031
show ip rip statistics ................................................................. 1032
shutdown ................................................................................. 1033

55  **Router Resources Commands** ................................................................. 1034
    system router resources ......................................................... 1034
    show system router resources ............................................... 1037

56  **DHCPv6 Commands** ........................................................................ 1039
    ipv6 dhcp client stateless ....................................................... 1039
    clear ipv6 dhcp client ............................................................ 1040
    ipv6 dhcp client information refresh ...................................... 1041
    ipv6 dhcp client information refresh minimum ......................... 1042
    ipv6 dhcp duid-en ................................................................. 1043
    ipv6 dhcp relay destination (Global) ....................................... 1044
    ipv6 dhcp relay destination (Interface) ..................................... 1046
    show ipv6 dhcp ................................................................... 1049
    show ipv6 dhcp interface ....................................................... 1051

57  **DHCP Server Commands** .................................................................. 1054
    ip dhcp server ................................................................. 1054
    ip dhcp pool host ............................................................... 1054
    ip dhcp pool network .......................................................... 1055
    address (DHCP Host) ........................................................... 1056
    address (DHCP Network) ...................................................... 1057
    lease ................................................................................. 1058
    client-name ................................................................. 1059
    default-router ................................................................. 1060
    dns-server ................................................................. 1061
    domain-name ................................................................. 1062
    netbios-name-server ......................................................... 1063
    netbios-node-type ............................................................. 1063
    next-server ................................................................. 1064
    next-server-name ............................................................. 1065
    bootfile ........................................................................... 1066
    time-server ................................................................. 1066
    option ............................................................................ 1067
    ip dhcp excluded-address .................................................... 1069
    clear ip dhcp binding ........................................................ 1070
    show ip dhcp .................................................................... 1071
    show ip dhcp excluded-addresses ........................................... 1072
    show ip dhcp pool host ....................................................... 1072
    show ip dhcp pool network .................................................. 1074
    show ip dhcp binding ........................................................ 1075
    show ip dhcp server statistics ................................................. 1077
    show ip dhcp allocated ........................................................ 1078
    show ip dhcp declined ........................................................ 1079
    show ip dhcp expired ........................................................ 1080
    show ip dhcp pre-allocated .................................................. 1081
58  UDLD Commands

show udld ................................................................. 1083
udld ................................................................. 1087
udld message time .................................................. 1088
udld port ............................................................... 1089

59  IPv6 First Hop Security

clear ipv6 first hop security counters .................................. 1093
clear ipv6 neighbor binding table ........................................ 1094
device-role (IPv6 DHCP Guard) ........................................ 1095
device-role (Neighbor Binding) .......................................... 1096
device-role (ND Inspection Policy) ...................................... 1097
device-role (RA Guard Policy) .......................................... 1099
drop-unsecure .......................................................... 1100
hop-limit ............................................................ 1101
ipv6 dhcp guard .......................................................... 1102
ipv6 dhcp guard attach-policy (port mode) .......................... 1103
ipv6 dhcp guard attach-policy (VLAN mode) ....................... 1106
ipv6 dhcp guard policy .................................................. 1107
ipv6 dhcp guard preference .............................................. 1109
ipv6 first hop security ................................................... 1111
ipv6 first hop security attach-policy (port mode) ................... 1112
ipv6 first hop security attach-policy (VLAN mode) ............... 1114
ipv6 first hop security logging packet drop .......................... 1115
ipv6 first hop security policy ............................................ 1116
ipv6 nd inspection ..................................................... 1117
ipv6 nd inspection attach-policy (port mode) ....................... 1119
ipv6 nd inspection attach-policy (VLAN mode) .................... 1121
ipv6 nd inspection drop-unsecure ...................................... 1122
ipv6 nd inspection policy .................................................. 1123
ipv6 nd inspection sec-level minimum ................................ 1125
ipv6 nd inspection validate source-mac .............................. 1126
ipv6 nd raguard ......................................................... 1127
ipv6 nd raguard attach-policy (port mode) ......................... 1128
ipv6 nd raguard attach-policy (VLAN mode) ....................... 1130
ipv6 nd raguard hop-limit .............................................. 1131
ipv6 nd raguard managed-config-flag ............................... 1132
ipv6 nd raguard other-config-flag .................................... 1133
ipv6 nd raguard policy .................................................. 1134
ipv6 nd raguard router-preference ..................................... 1137
ipv6 neighbor binding ................................................... 1138
ipv6 neighbor binding attach-policy (port mode) .................. 1139
ipv6 neighbor binding attach-policy (VLAN mode) ............... 1141
ipv6 neighbor binding lifetime ......................................... 1142
ipv6 neighbor binding logging ......................................... 1143
ipv6 neighbor binding max-entries .................................... 1144
ipv6 neighbor binding policy ............................................ 1145
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor binding static</td>
<td>1147</td>
</tr>
<tr>
<td>logging binding</td>
<td>1148</td>
</tr>
<tr>
<td>logging packet drop</td>
<td>1149</td>
</tr>
<tr>
<td>managed-config-flag</td>
<td>1150</td>
</tr>
<tr>
<td>match ra address</td>
<td>1151</td>
</tr>
<tr>
<td>match ra prefixes</td>
<td>1153</td>
</tr>
<tr>
<td>match reply</td>
<td>1154</td>
</tr>
<tr>
<td>match server address</td>
<td>1155</td>
</tr>
<tr>
<td>max-entries</td>
<td>1157</td>
</tr>
<tr>
<td>other-config-flag</td>
<td>1158</td>
</tr>
<tr>
<td>preference</td>
<td>1159</td>
</tr>
<tr>
<td>router-preference</td>
<td>1161</td>
</tr>
<tr>
<td>sec-level minimum</td>
<td>1162</td>
</tr>
<tr>
<td>show ipv6 dhcp guard</td>
<td>1163</td>
</tr>
<tr>
<td>show ipv6 dhcp guard policy</td>
<td>1164</td>
</tr>
<tr>
<td>show ipv6 first hop security</td>
<td>1165</td>
</tr>
<tr>
<td>show ipv6 first hop security active policies</td>
<td>1166</td>
</tr>
<tr>
<td>show ipv6 first hop security attached policies</td>
<td>1168</td>
</tr>
<tr>
<td>show ipv6 first hop security counters</td>
<td>1169</td>
</tr>
<tr>
<td>show ipv6 nd inspection</td>
<td>1171</td>
</tr>
<tr>
<td>show ipv6 nd inspection policy</td>
<td>1171</td>
</tr>
<tr>
<td>show ipv6 nd raguard</td>
<td>1173</td>
</tr>
<tr>
<td>show ipv6 nd raguard policy</td>
<td>1174</td>
</tr>
<tr>
<td>show ipv6 neighbor binding</td>
<td>1175</td>
</tr>
<tr>
<td>show ipv6 neighbor binding policy</td>
<td>1176</td>
</tr>
<tr>
<td>show ipv6 neighbor binding table</td>
<td>1177</td>
</tr>
<tr>
<td>validate source-mac</td>
<td>1179</td>
</tr>
</tbody>
</table>
Summary of New/Modified Features for 500 Family, Release 1.3.7

Table 1 describes the CLI commands that were added/modified to release 1.3.7 after release 1.3.5.

Table 1: New/Modified 1.3.5 Commands

<table>
<thead>
<tr>
<th>CLI Chapter</th>
<th>CLI Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE</td>
<td>power inline legacy support disable</td>
<td>New</td>
</tr>
</tbody>
</table>
Introduction

This section describes how to use the Command Line Interface (CLI). It contains the following topics:

- User (Privilege) Levels
- CLI Command Modes
- Accessing the CLI
- CLI Command Conventions
- Editing Features
- Interface Naming Conventions
- System Modes
- Loopback Interface

Overview

The CLI is divided into various command modes. Each mode includes a group of commands. These modes are described in CLI Command Modes.

Users are assigned privilege levels. Each user privilege level can access specific CLI modes. User levels are described in the section below.

User (Privilege) Levels

Users can be created with one of the following user levels:

- **Level 1**—Users with this level can only run User EXEC mode commands. Users at this level cannot access the web GUI or commands in the Privileged EXEC mode.

- **Level 7**—Users with this level can run commands in the User EXEC mode and a subset of commands in the Privileged EXEC mode. Users at this level cannot access the web GUI.
• **Level 15**—Users with this level can run all commands. Only users at this level can access the web GUI.

A system administrator (user with level 15) can create passwords that allow a lower level user to temporarily become a higher level user. For example, the user may go from level 1 to level 7, level 1 to 15, or level 7 to level 15.

The passwords for each level are set (by an administrator) using the following command:

```
enable password [level privilege-level] {password | encrypted encrypted-password}
```

Using these passwords, you can raise your user level by entering the command: `enable` and the password for level 7 or 15. You can go from level 1 to level 7 or directly to level 15. The higher level holds only for the current session.

The `disable` command returns the user to a lower level.

To create a user and assign it a user level, use the `username` command. Only users with command level 15, can create users at this level.

Example—Create passwords for level 7 and 15 (by the administrator):

```
switchxxxxxx#configure
switchxxxxxx<conf># enable password level 7 level7@abc
switchxxxxxx<conf># enable password level 15 level15@abc
switchxxxxxx<conf>#
```

Create a user with user level 1:

```
switchxxxxxx#configure
switchxxxxxx<conf> username john password john1234 privilege 1
switchxxxxxx<conf>
```
Example 2—Switch between Level 1 to Level 15. The user must know the password:

```bash
switchxxxxxx#
switchxxxxxx# enable
Enter Password: ****** (this is the password for level 15 - level15@abc)
switchxxxxxx#
```

**NOTE** If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 7 and user level 15 must be configured on the external server and associated with the $enable7$ and $enable15$ user names, respectively. See the Authentication, Authorization and Accounting (AAA) Commands chapter for details.

### CLI Command Modes

The CLI is divided into four command modes. The command modes are (in the order in which they are accessed):

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode
- Interface Configuration mode

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode and for the level of the user. Specific commands are used to switch from one mode to another.

Users are assigned privilege levels that determine the modes and commands available to them. User levels are described in **User (Privilege) Levels**.

### User EXEC Mode

Users with level 1 initially log into User EXEC mode. User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.
The user-level prompt consists of the switch host name followed by a #. The default host name is `switchxxxxxx` where `xxxxxx` is the last six digits of the device’s MAC address, as shown below.

```
switchxxxxxx#
```

The default host name can be changed via the `hostname` command in Global Configuration mode.

**Privileged EXEC Mode**

A user with level 7 or 15 automatically logs into Privileged EXEC mode.

Users with level 1 can enter Privileged Exec mode by entering the `enable` command, and when prompted, the password for level 15.

To return from the Privileged EXEC mode to the User EXEC mode, use the `disable` command.

**Global Configuration Mode**

The Global Configuration mode is used to run commands that configure features at the system level, as opposed to the interface level.

Only users with command level of 7 or 15 can access this mode.

To access Global Configuration mode from Privileged EXEC mode, enter the `configure` command at the Privileged EXEC mode prompt and press `Enter`. The Global Configuration mode prompt, consisting of the device host name followed by `(config)#`, is displayed:

```
switchxxxxxx(config)#
```

Use any of the following commands to return from Global Configuration mode to the Privileged EXEC mode:

- `exit`
- `end`
- `Ctrl+Z`
The following example shows how to access Global Configuration mode and return to Privileged EXEC mode:

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# exit
switchxxxxxx#
```

**Interface or Line Configuration Modes**

Various submodes may be entered from Global Configuration mode. These submodes enable performing commands on a group of interfaces or lines.

For instance to perform several operations on a specific port or range of ports, you can enter the Interface Configuration mode for that interface.

The following example enters Interface Configuration mode for ports gi1-5 and then sets their speed:

The `exit` command returns to Global Configuration mode.

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# interface range gi1/1/1-5
switchxxxxxx(config-if)# speed 10
switchxxxxxx(config-if)# exit
switchxxxxxx(config)#
```

The following submodes are available:

- **Interface**—Contains commands that configure a specific interface (port, VLAN, port channel, or tunnel) or range of interfaces. The Global Configuration mode command `interface` is used to enter the Interface
Configuration mode. The `interface` Global Configuration command is used to enter this mode.

- **Line Interface**—Contains commands used to configure the management connections for the console, Telnet and SSH. These include commands such as line timeout settings, etc. The `line` Global Configuration command is used to enter the Line Configuration command mode.

- **VLAN Database**—Contains commands used to configure a VLAN as a whole. The `vlan database` Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.

- **Management Access List**—Contains commands used to define management access-lists. The `management access-list` Global Configuration mode command is used to enter the Management Access List Configuration mode.

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

- **QoS**—Contains commands related to service definitions. The `qos` Global Configuration mode command is used to enter the QoS services configuration mode.

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

To return from any Interface Configuration mode to the Global Configuration mode, use the `exit` command.

## Accessing the CLI

The CLI can be accessed from a terminal or computer by performing one of the following tasks:

- Running a terminal application, such as HyperTerminal, on a computer that is directly connected to the switch’s console port,

  —or—
• Running a Telnet session from a command prompt on a computer with a network connection to the switch.

• Using SSH.

**NOTE** Telnet and SSH are disabled by default on the switch.

If access is via a Telnet connection, ensure that the following conditions are met before using CLI commands:

• The switch has a defined IP address.

• Corresponding management access is granted.

• There is an IP path such that the computer and the switch can reach each other.

### Using HyperTerminal over the Console Interface

The switch's RS-232 serial console port provides a direct connection to a computer's serial port using a standard DB-9 null-modem or crossover cable. After the computer and switch are connected, run a terminal application to access the CLI.

Click Enter twice, so that the device sets the serial port speed to match the PC's serial port speed.

When the `CLI` appears, enter `cisco` at the *User Name* prompt and press **Enter**.

The switchxxxxxx# prompt is displayed. You can now enter CLI commands to manage the switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this reference guide.

### Using Telnet over an Ethernet Interface

Telnet provides a method of connecting to the CLI over an IP network.

To establish a telnet session from the command prompt, perform the following steps:
STEP 1 Click Start, then select All Programs > Accessories > Command Prompt to open a command prompt.

Figure 1 Start > All Programs > Accessories > Command Prompt

STEP 2 At the prompt, enter telnet 1<IP address of switch>, then press Enter.

Figure 2 Command Prompt

STEP 3 The CLI will be displayed.

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>In a command line, square brackets indicate an optional entry.</td>
</tr>
<tr>
<td>{ }</td>
<td>In a command line, curly brackets indicate a selection of compulsory parameters separated the</td>
</tr>
<tr>
<td>parameter</td>
<td>Italic text indicates a parameter.</td>
</tr>
</tbody>
</table>
### Editing Features

#### Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command `show interfaces status Gigabitethernet 1`, `show`, `interfaces` and `status` are keywords, `Gigabitethernet` is an argument that specifies the interface type, and `1` specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
switchxxxxxx(config)# username admin password alansmith
```

When working with the CLI, the command options are not displayed. The standard command to request help is `?`.

### Table: Convention

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>press key</td>
<td>Names of keys to be pressed are shown in <strong>bold</strong>.</td>
</tr>
<tr>
<td>Ctrl+F4</td>
<td>Keys separated by the + character are to be pressed simultaneously on the keyboard.</td>
</tr>
<tr>
<td>Screen Display</td>
<td>Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed on the console.</td>
</tr>
<tr>
<td>all</td>
<td>When a parameter is required to define a range of ports or parameters and all is an option, the default for the command is <strong>all</strong> when no parameters are defined. For example, the command <code>interface range port-channel</code> has the option of either entering a range of channels, or selecting all. When the command is entered without a parameter, it automatically defaults to all.</td>
</tr>
<tr>
<td>text</td>
<td>When free text is entered as a parameter for a command, it must be entered between double quotes in the following cases:</td>
</tr>
<tr>
<td></td>
<td>- If the text consists of multiple words separated by blanks, the entire string must appear in double quotes. For example: <code>snmp-server contact &quot;QA on floor 8&quot;</code></td>
</tr>
<tr>
<td></td>
<td>- If the text is the name of a Layer 2 interface (port, port-channel or VLAN). For example: <code>ipv6 nd inspection policy &quot;po 1&quot;</code>.</td>
</tr>
</tbody>
</table>
There are two instances where help information can be displayed:

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

- **Partial keyword lookup**—If a command is incomplete and or the character `?` is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- **Terminal Command Buffer**
- **Command Completion**
- **Interface Naming Conventions**
- **Keyboard Shortcuts**

### Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-Arrow key</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl+P</td>
<td></td>
</tr>
<tr>
<td>Down-Arrow key</td>
<td>Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.</td>
</tr>
</tbody>
</table>

By default, the history buffer system is enabled, but it can be disabled at any time. For more information on enabling or disabling the history buffer, refer to the **history** command.
There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For more information on configuring the command history buffer, refer to the `history size` command.

To display the history buffer, refer to the `show history` command.

**Negating the Effect of Commands**

For many configuration commands, the prefix keyword `no` can be entered to cancel the effect of a command or reset the configuration to the default value. This Reference Guide provides a description of the negation effect for each CLI command.

**Command Completion**

If the command entered is incomplete, invalid or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing `Tab` after an incomplete command is entered, the system will attempt to identify and complete the command. If the characters already entered are not enough for the system to identify a single matching command, press `?` to display the available commands matching the characters already entered.

**Keyboard Shortcuts**

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

<table>
<thead>
<tr>
<th>Keyboard Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-arrow</td>
<td>Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Down-arrow</td>
<td>Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.</td>
</tr>
<tr>
<td>Ctrl+A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
</tbody>
</table>
Introduction

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.

**NOTE**

It is the user’s responsibility to ensure that the text copied into the device consists of legal commands only.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.

The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device except for encrypted passwords where the keyword encrypted is used before the encrypted data (for instance in the `enable password` command).

Interface Naming Conventions

**Interface ID**

Within the CLI, interfaces are denoted by concatenating the following elements:

- **Type of Interface** — The following types of interfaces are found on the various types of devices:
  - **(For supporting devices only) FastEthernet (10/100 bits) ports** — This can be written as `FastEthernet`, `fa` or `fe`.
  - **GigabitEthernet ports (10/100/1000 bits) ports** — This can be written as either `GigabitEthernet` or `gi` or `GE`. For SG500XG devices, there is a single port of this type for each unit.
  - **TenGigabit thernet ports (10000 bits) ports** — This can be written as either `TenGigabitEthernet` or `te` or `xg`.

---

### Keyboard Key | Description

<table>
<thead>
<tr>
<th>Ctrl+E</th>
<th>Moves the cursor to the end of the command line.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+Z / End</td>
<td>Returns back to the Privileged EXEC mode from any configuration mode.</td>
</tr>
<tr>
<td>Backspace</td>
<td>Deletes one character left to the cursor position.</td>
</tr>
</tbody>
</table>
- **LAG (Port Channel)**—This can be written as either **Port-Channel** or **po**.
- **VLAN**—This is written as **VLAN**
- **Tunnel**—This is written as **tunnel** or **tu**

- **Unit Number**—Unit in stack. In standalone models this is always 1 (1 by default)

- **Slot Number for Sx500 devices**—The slot number is either 1 or 2; 1 for GigabitEthernet ports and 2 for FastEthernet ports.

- **Slot Number for SG500X devices**—The slot number is always 1.

- **Slot Number for SG500XG devices**—The slot number is always 2.

  The syntax for interface names in stacking mode is:

  \[
  \{<port-type>[ ][<unit-number>/]<slot-number>/<port-number>\} \ |
  \{port-channel | po | ch\}[ ][<port-channel-number> ] l
  \{tunnel | tu\}[ ][<tunnel-number> ] l vlan[ ]<vlan-id>
  \]

- **Interface Number**—Port, LAG, tunnel or VLAN ID

Sample of these various options are shown in the example below:

```
switchxxxxxx(config)#interface GigabitEthernet 1/1/1
switchxxxxxx(config)#interface GE 1/1/1
switchxxxxxx(config)#interface FastEthernet 1/2/1
switchxxxxxx((config)#interface fe1/2/1
switchxxxxxx((config)#interface tel/2/1
switchxxxxxx(config)#interface po1
switchxxxxxx(config)# interface vlan 1
```

**NOTE**  See **Loopback Interface** for a description of the loopback interface.

## Interface Range

Interfaces may be described on an individual basis or within a range. The interface range command has the following syntax:

\[
<interface-range> ::= 
\]
A sample of this command is shown in the example below:

```
switchxxxxxx#configure
switchxxxxxx(config-if)#interface range gi1/1/1-1/1/5
```

### Interface List

A combination of interface types can be specified in the `interface range` command in the following format:

```
<range-list> ::= <interface-range> | <range-list>, <interface-range>
```

Up to five ranges can be included.

**NOTE**

Range lists can contain either ports and port-channels or VLANs. Combinations of port/port-channels and VLANs are not allowed.

The space after the comma is optional.

When a range list is defined, a space after the first entry and before the comma (,) must be entered.

A sample of this command is shown in the example below:

```
switchxxxxxx#configure
switchxxxxxx(config)#interface range gi1/1/1-1/1/5, vlan 1-2
```
IPv6z Address Conventions

The following describes how to write an IPv6z address, which is a link-local IPv6 address.

The format is: `<ipv6-link-local-address>%<egress-interface>

where:

**egress-interface** (also known as zone) = vlan<vlan-id> \| po<number> \| tunnel<number> \| port<number> \| 0

If the egress interface is not specified, the default interface is selected. Specifying egress interface = 0 is equal to not defining an egress interface.

The following combinations are possible:

- **ipv6_address%egress-interface** — Refers to the IPv6 address on the interface specified.

- **ipv6_address%0** — Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

- **ipv6_address** — Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

System Modes

Sx500 devices function in either Router (Layer 3) or Switch (Layer 2) system mode, while SG500X and SG500XG devices always function in Switch plus Router system mode. Therefore, the parts of this section that refer to switching between the two system modes are not relevant for SG500X and SG500XG devices.

When stacking the SG500X with Sx500 in one of the Hybrid stack modes, the system mode must also be defined, and is valid for both Sx500 and SG500X.

The default mode is Switch system mode. To change the system mode of the switch to Router, use the **set system** command.

This command performs a system reboot.

In Switch system mode, the switch forwards packets as a VLAN-aware bridge. In Router system mode, the switch performs both IPv4 routing and VLAN-aware bridging.
If Router system mode is selected, a single IP address is supported on the default VLAN. The user also must configure a default gateway.

If Switch system mode is selected, the user can manage the device on any IP interface configured on the device, as long as a default route is configured. In Router system mode, the switch routes traffic between IP VLANs, and bridges traffic within VLANs.

When the switch operates in Router system mode, the following features are not supported:

- Protocol-based VLANs
- MAC-based VLANs
- DVA, Multicast TV VLAN
- Per flow policing

## Loopback Interface

When an IP application on a router wants to communicate with a remote IP application, it must select the local IP address to be used as its IP address. It can use any IP address defined on the router, but if this link goes down, the communication is aborted, even though there might well be another IP route between these IP applications.

The loopback interface is a virtual interface whose operational state is always up. If the IP address that is configured on this virtual interface is used as the local address when communicating with remote IP applications, the communication will not be aborted even if the actual route to the remote application was changed.

The name of the loopback interface is `loopback1`.

A loopback interface does not support bridging; it cannot be a member of any VLAN, and no layer 2 protocol can be enabled on it.

## Layer 3 Specification

### IP Interface

IPv4 and IPv6 addresses can be assigned to a loopback interface.

The IPv6 link-local interface identifier is 1.
Routing Protocols

A routing protocol running on the switch supports the advertising of the IP prefixes defined on the loopback interfaces via the routing protocol redistribution mechanism.

If a layer 2 switch with one IPv4 address supports a loopback interface, the above rules are replaced by the following ones:

This is the definition of the IP configuration when the device is in layer 2 mode:

- Only one loopback interface is supported.
- Two IPv4 interfaces can be configured: one on a VLAN and one on the loopback interface.
- If the IPv4 address was configured on the default VLAN and the default VLAN is changed, the switch moves the IPv4 address to the new default VLAN.
- The `ip address` command does the following:
  - In VLAN context, it replaces the existing configured IPv4 address on the specified interface by the new one.
  - In VLAN context, it supports the keyword `default-gateway`.
  - In Loopback Interface context, it replaces the existing, configured IPv4 address on the loopback interface with the new one.
  - In the Loopback Interface context, it does not support the keyword `default-gateway`. 
Configuration Examples

Layer 2 Switch

The following example shows how to configure IP on a Layer 2 switch:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
default-gateway 10.10.10.1
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# ipv6 address
2001:DB8:2222:7272::.72/128
Switch(config-if)# exit
```

The router with IP Address 10.10.10.1 should be configured with the following static route: ip route 172.25.13.2 /32 10.10.10.2.
Layer 3 Switch with Static Routing

The following example shows you how to configure IP on a Layer 3 switch with static routing:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
Switch(config-if)# ipv6 address 2001:DB8:2222:7270::2312/64
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.11.11.2 /24
Switch(config-if)# ipv6 address 2001:DB8:3333:7271::2312/64
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# ipv6 address 2001:DB8:2222:7272::72/128
Switch(config-if)# exit
Switch(config)# ip route 0.0.0.0/0 10.10.11.1
Switch(config)# ip route 10.11.0.0 /16 10.11.11.1
Switch(config)# ipv6 route 0::/0  2001:DB8:2222:7270::1
Switch(config)# ipv6 route 2001:DB8:3333::/48
    2001:DB8:3333:7271::1
```

The neighbor router 10.10.11.1 should be configured with the following static route: ip route 172.25.13.2 /32 10.10.10.2.

The neighbor router 10.11.11.1 should be configured with the following static route: ip route 172.25.13.2 /32 10.11.11.2.

The neighbor router 2001:DB8:2222:7270::1 connected to VLAN 1 should be configured with the following static route:

```
ipv6 route 2001:DB8:2222:7272::72/128 2001:DB8:2222:7270::2312
```
The neighbor router 2001:DB8:3333:7271::1 connected to VLAN 1 should be configured with the static route defined immediately below.


**Without RIP on the Loopback Interface**

The following example describes how to configure IP on a Layer 3 switch with RIP not running on the loopback interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.11.11.2 /24
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-rip)# network 10.10.10.2
Switch(config-rip)# network 10.11.10.2
Switch(config-rip)# redistribute connected
Switch(config-rip)# exit
```

The other routers need static routes for 172.25.13.2/32, because the route is advertised by RIP.
With RIP on the Loopback Interface

The following example describes how to configure IP on a Layer 3 switch with RIP running on the loopback interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.11.11.2 /24
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-rip)# network 10.10.10.2
Switch(config-rip)# network 10.11.10.2
Switch(config-rip)# network 172.25.13.2
Switch(config-rip)# exit
Switch(config)# interface ip 172.25.13.2
Switch(config-ip)# ip rip passive-interface
Switch(config-ip)# exit
```

The other routers do not need static routes for 172.25.13.2/32, because the route is advertised by RIP.
User Interface Commands

3.1 enable

The enable EXEC mode command enters the Privileged EXEC mode.

Syntax

```
enable [privilege-level]
```

Parameters

- `privilege-level`—Specifies the privilege level at which to enter the system. (Range: 1, 7, 15)

Default Configuration

The default privilege level is 15.

Command Mode

EXEC mode

Example

The following example enters privilege level 7.

```
switchxxxxxx# enable 7
enter password:**********
switchxxxxxx# Accepted
```

The following example enters privilege level 15.

```
switchxxxxxx# enable
enter password:**********
switchxxxxxx# Accepted
```
3.2  disable

The **disable** Privileged EXEC mode command leaves the Privileged EXEC mode and returns to the User EXEC mode.

**Syntax**

```
disable [privilege-level]
```

**Parameters**

- **privilege-level**—Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to 1.

**Default Configuration**

The default privilege level is 1.

**Command Mode**

Privileged EXEC mode

**Example**

The following example returns the user to user level 1.

```
switchxxxxxx# disable 1
switchxxxxxx#
```

3.3  login

The **login** EXEC mode command enables changing the user that is logged in. When this command is logged in, the user is prompted for a username/password.

**Syntax**

```
login
```

**Parameters**

- **N/A**
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example enters Privileged EXEC mode and logs in with the required username ‘bob’.

switchxxxxxx# login
User Name: bob
Password: *****
switchxxxxxx#

3.4 configure
The configure Privileged EXEC mode command enters the Global Configuration mode.

Syntax
configure [terminal]

Parameters
terminal—Enter the Global Configuration mode with or without the keyword terminal.

Command Mode
Privileged EXEC mode

Example
The following example enters Global Configuration mode.

switchxxxxxx# configure
switchxxxxxx(config)#
3.5  **exit (Configuration)**

The `exit` command exits any mode and brings the user to the next higher mode in the CLI mode hierarchy.

**Syntax**

```
exit
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

All.

**Examples**

The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
```

3.6  **exit (EXEC)**

The `exit` EXEC mode command closes an active terminal session by logging off the device.

**Syntax**

```
exit
```

**Parameters**

N/A
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example closes an active terminal session.

```text
switchxxxxxx# exit
```

### 3.7 end

The `end` command ends the current configuration session and returns to the Privileged EXEC mode.

**Syntax**

`end`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

All

**Example**

The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode.

```text
switchxxxxxx(config)# end
switchxxxxxx#
```
3.8 help

The help command displays a brief description of the Help system.

Syntax
help

Parameters
N/A

Default Configuration
N/A

Command Mode
All

Example
The following example describes the Help system.

switchxxxxxx# help

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches the currently entered incomplete command, the help list is empty. This indicates that there is no command matching the input as it currently appears. If the request is within a command, press the Backspace key and erase the entered characters to a point where the request results in a match.

Help is provided when:

1. There is a valid command and a help request is made for entering a parameter or argument (e.g. 'show ?'). All possible parameters or arguments for the entered command are then displayed.

2. An abbreviated argument is entered and a help request is made for arguments matching the input (e.g. 'show pr?').
### 3.9 history

The `history` Line Configuration mode command enables saving commands that have been entered. Use the `no` form of this command to disable the command.

**Syntax**

```
history
no history
```

**Parameters**

N/A

**Default Configuration**

Enabled.

**Command Mode**

Line Configuration mode

**User Guidelines**

This command enables saving user-entered commands for a specified line. You can return to previous lines by using the up or down arrows.

It is effective from the next time that the user logs in via console/telnet/ssh.

The following are related commands:

- Use the `terminal history size` EXEC mode command to enable or disable this command for the current terminal session.
- Use the `history size` Line Configuration mode command to set the size of the command history buffer.

**Example**

The following example enables the command for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history
```
3.10 history size

The history size Line Configuration mode command changes the maximum number of user commands that are saved in the history buffer for a particular line. Use the no form of this command to reset the command history buffer size to the default value.

Syntax

```
history size number-of-commands

no history size
```

Parameters

`number-of-commands`—Specifies the number of commands the system records in its history buffer.

Default Configuration

The default command history buffer size is 10 commands.

Command Mode

Line Configuration mode

User Guidelines

This command configures the command history buffer size for a particular line. It is effective from the next time that the user logs in via console/telnet/ssh.

Use the `terminal history size` EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size cannot be increased above the default size.

Example

The following example changes the command history buffer size to 100 entries for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history size 100
```
3.11 terminal history

The terminal history EXEC mode command enables the command history function for the current terminal session, meaning it is not stored in the Running Configuration file. Use the no form of this command to disable the command.

Syntax

terminal history

terminal no history

Default Configuration

The default configuration for all terminal sessions is defined by the history Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history Line Configuration mode command.

This command is effective immediately.

Example

The following example disables the command history function for the current terminal session.

switchxxxxxx# terminal no history

3.12 terminal history size

The terminal history size EXEC mode command changes the command history buffer size for the current terminal session, meaning it is not stored in the Running Configuration file. Use the no form of this command to reset the command history buffer size to the default value.

Syntax

terminal history size number-of-commands
terminal no history size

Parameters

number-of-commands—Specifies the number of commands the system maintains in its history buffer. (Range: 10–207)

Default Configuration

The default configuration for all terminal sessions is defined by the history size Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The terminal history size EXEC command changes the command history buffer size for the current terminal session. Use the history Line Configuration mode command to change the default history buffer size.

The maximum number of commands in all buffers is 207.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
switchxxxxxx#terminal history size 20
```

3.13 terminal datadump

The terminal datadump EXEC mode command enables dumping all the output of a show command without prompting. Use the no form of this command to disable dumping.

Syntax

terminal datadump

terminal no datadump

Parameters

N/A
Default Configuration
When printing, dumping is disabled and printing is paused every 24 lines.

Command Mode
EXEC mode

User Guidelines
By default, a More prompt is displayed when the output contains more than 24 lines. Pressing the Enter key displays the next line; pressing the Spacebar displays the next screen of output.

The terminal datadump command enables dumping all output immediately after entering the show command by removing the pause.

The width is not limited, and the width of the line being printed on the terminal is based on the terminal itself.

This command is relevant only for the current session.

Example
The following example dumps all output immediately after entering a show command.

```
switchxxxxxx# terminal datadump
```

3.14 terminal width
Use the terminal width EXEC mode command to determine the width of the display for the echo input to CLI sessions. Use terminal no width to return to the default.

The command is per session and will not be saved in the configuration database.

Syntax

```
terminal width number-of-characters
terminal no width
```
Parameters

**number-of-characters** - Specifies the number of characters to be displayed for the echo output of the CLI commands and the configuration file. '0' means endless number of characters on a screen line. (Range: 0, 70-512)

**Default Configuration**

The default number of characters is 77.

**Command Mode**

Privileged EXEC mode

**Example**

The following example sets the terminal width to 100 characters

```
switchxxxxxx# terminal width 100
```

### 3.15 terminal prompt

Use the `terminal prompt` EXEC mode command to enable the terminal prompts. Use `terminal no prompt` command to disable the terminal prompts.

The command is per session and will not be saved in the configuration database.

**Syntax**

```
terminal prompt
terminal no prompt
```

**Parameters**

N/A

**Default Configuration**

The default configuration is prompts enabled.

**Command Mode**

Privileged EXEC mode
Example
The following example disables the terminal prompts

switchxxxxxx# terminal no prompt

3.16  show history

The show history EXEC mode command lists commands entered in the current session.

Syntax
show history

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

User Guidelines
The buffer includes executed and unexecuted commands. Commands are listed from the first to the most recent command. The buffer remains unchanged when entering into and returning from configuration modes.

Example
The following example displays all the commands entered while in the current Privileged EXEC mode.

switchxxxxxx# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
switchxxxxxx# show clock
3.17 **show privilege**

The **show privilege** EXEC mode command displays the current privilege level.

**Syntax**

```
show privilege
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays the privilege level for the user logged on.

```
switchxxxxxx# show privilege
Current privilege level is 15
```

3.18 **do**

The **do** command executes an EXEC-level command from Global Configuration mode or any configuration submode.
Syntax

`do command`

Parameters

command—Specifies the EXEC-level command to execute.

Command Mode

All configuration modes

Example

The following example executes the `show vlan` Privileged EXEC mode command from Global Configuration mode.

```
switchxxxxxx(config)# do show vlan

Vlan  Name        Ports                   Type         Authorization
---- ----        ---------------------    --------     -------------
  1    1           gi1/1/1-39,Po1,Po2,         other        Required
  2    2           gi1/1/1                     dynamicGvtp  Required
 10   v0010       gi1/1/1                     permanent    Not Required
 11   V0011       gi1/1/1,gi1/1/3             permanent    Required
 20   20          gi1/1/1                     permanent    Required
 30   30          gi1/1/1,gi1/1/3             permanent    Required
 31   31          gi1/1/1                     permanent    Required
 91   91          gi1/1/1,gi1/1/4             permanent    Required
4093 guest-vlan  gi1/1/1,gi1/1/3             permanent    Guest

switchxxxxxx(config)#
```

3.19 banner exec

Use the `banner exec` Global Configuration mode command to specify and enable a message to be displayed after a successful logon. This banner is applied automatically on all the user interfaces: console, Telnet and SSH and also on the WEB GUI. Use the `no` form of this command to delete the existing EXEC banner.
Syntax

```
banner exec d message-text d
no banner exec
```

Parameters

- **d**—Delimiting character of user’s choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

- **message-text**—The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of $(token) in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, press <Enter> to continue).

Default Configuration

Disabled (no EXEC banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of $(token) in the message text to customize the banner. The tokens are described in the table below:

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name for the device.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name for the device.</td>
</tr>
<tr>
<td>$(bold)</td>
<td>Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.</td>
</tr>
<tr>
<td>$(inverse)</td>
<td>Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.</td>
</tr>
<tr>
<td>$(contact)</td>
<td>Displays the system contact string.</td>
</tr>
<tr>
<td>$(location)</td>
<td>Displays the system location string.</td>
</tr>
</tbody>
</table>
Use the **no banner exec** Line Configuration command to disable the Exec banner on a particular line or lines.

**Example**

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the $(token)$ syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner exec %
Enter TEXT message. End with the character '%'.
$(bold)Session activated.$(bold) Enter commands at the prompt.
%
```

When a user logs on to the system, the following output is displayed:

```
Session activated. Enter commands at the prompt.
```

### 3.20 **banner login**

Use the **banner login** command in Global Configuration mode to specify a message to be displayed before the username and password login prompts. This banner is applied automatically on all the user interfaces: Console, Telnet and SSH and also on the WEB GUI. Use the **no** form of this command to delete the existing login banner.

**Syntax**

```
banner login d message-text d

no banner login
```

**Parameters**

- **d**—Delimiting character of user’s choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

- **message-text**—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of $(token)$ in the message text. Tokens are replaced with the corresponding

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(mac-address)</td>
<td>Displays the base MAC address of the device.</td>
</tr>
</tbody>
</table>
configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, you must press <Enter> to continue).

**Default Configuration**

Disabled (no Login banner is displayed).

**Command Mode**

Global Configuration mode

**User Guidelines**

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of $(token) in the message text to customize the banner. The tokens are described in the table below:

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name for the device.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name for the device.</td>
</tr>
<tr>
<td>$(bold)</td>
<td>Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.</td>
</tr>
<tr>
<td>$(inverse)</td>
<td>Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.</td>
</tr>
<tr>
<td>$(contact)</td>
<td>Displays the system contact string.</td>
</tr>
<tr>
<td>$(location)</td>
<td>Displays the system location string.</td>
</tr>
<tr>
<td>$(mac-address)</td>
<td>Displays the base MAC address of the device.</td>
</tr>
</tbody>
</table>

Use the **no banner login** Line Configuration command to disable the Login banner on a particular line or lines.

**Example**

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the $(token) syntax is replaced by the corresponding configuration variable.
switchxxxxxx(config)# banner login %
Enter TEXT message. End with the character '%'.

You have entered $(hostname).$(domain)
%

When the login banner is executed, the user will see the following banner:

You have entered host123.ourdomain.com

3.21 show banner

Use the show banner commands in EXEC mode to display the banners that have been defined.

Syntax

show banner login
show banner exec

Parameters

N/A

Command Mode

EXEC mode

Examples

switchxxxxxx# show banner login

-------------------------------------------------------------
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
## Macro Commands

### 4.1 macro name

Use the **macro name** Global Configuration mode command to define a macro. There are two types of macros that can be defined:

- Global macros define a group of CLI commands that can be run at any time.
- Smartport macros are associated with Smartport types (**Smartport Commands**). For each Smartport macro there must be an anti macro (a macro whose name is concatenated with **no_**). The anti macro reverses the action of the macro.

If a macro with this name already exists, it overrides the previously-defined one. Use the **no** form of this command to delete the macro definition.

**Syntax**

```
macro name [macro-name]
no macro name [macro-name]
```

**Parameters**

- **macro-name**—Name of the macro. Macro names are case sensitive.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**User Guidelines**

A macro is a script that contains CLI commands and is assigned a name by the user. It can contain up to 3000 characters and 200 lines.

**Keywords**

Macros may contain keywords (parameters). The following describes keywords:
A macro can contain up to three keywords.

All matching occurrences of the keyword are replaced by the corresponding value specified in the macro.

Keyword matching is case-sensitive.

Applying a macro with keywords does not change the state of the original macro definition.

User Feedback

The behavior of a macro command requiring user feedback is the same as if the command is entered from terminal: it sends its prompt to the terminal and accepts the user reply.

Creating a Macro

Use the following guidelines to create a macro:

- Use `macro name` to create the macro with the specified name.
- Enter one macro command per line.
- Use the `@` character to end the macro.
- Use the `#` character at the beginning of a line to enter a comment in the macro.

In addition, `#` is used to identify certain preprocessor commands that can only be used within a macro. There are two possible preprocessor commands:

- `#macro key description` - Each macro can be configured with up to 3 keyword/description pairs. The keywords and descriptions are displayed in the GUI pages when the macro is displayed.

  The syntax for this preprocessor command is as follows:

  `#macro key description $keyword1 description1 $keyword2 description2 $keyword3 description3`

  A keyword must be prefixed with `$`.

- `#macro keywords` - This instruction enables the device to display the keywords as part of the CLI help. It accepts up to 3 keywords. The command creates a CLI help string with the keywords for the macro. The help string will be displayed if help on the macro is requested from the `macro` and `macro global` commands. The GUI also uses the keywords specified in the command as the parameter names for the macro. See
Example 2 and 3 below for a description of how this command is used in the CLI.

The syntax for this preprocessor command is as follows:

```
#macro keywords $keyword1 $keyword2 $keyword3
```

where $keywordn is the name of the keyword.

**Editing a Macro**

Macros cannot be edited. Modify a macro by creating a new macro with the same name as the existing macro. The newer macro overwrites the existing macro.

The exceptions to this are the built-in macros and corresponding anti-macros for the Smartport feature. You cannot override a Smartport macro. To change a Smartport macro, create a new macro (my_macro) and an anti macro (no_my_macro) and associate it with the Smartport type using macro auto user smartport macro.

**Scope of Macro**

It is important to consider the scope of any user-defined macro. Because of the potential hazards of applying unintended configurations, do not change configuration modes within the macro by using commands such as exit, end, or interface interface-id. With a few exceptions, there are other ways of executing macros in the various configuration modes. Macros may be executed in Privileged Exec mode, Global Configuration mode, and Interface Configuration mode (when the interface is NOT a VLAN.)

**Examples**

**Example 1** -The following example shows how to create a macro that configures the duplex mode of a port.

```
switchxxxxxx(config)#  macro name dup
Enter macro commands one per line. End with the character '\@'.
#macro description dup
duplex full
negotiation
@
```

**Example 2** -The following example shows how to create a macro with the parameters: DUPLEX and SPEED. When the macro is run, the values of DUPLEX
and SPEED must be provided by the user. The \#macro keywords command enables the user to receive help for the macro as shown in Example 3.

```
switchxxxxxx(config) # macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex $DUPLEX
no negotiation
speed $SPEED
#macro keywords $DUPLEX $SPEED
@
```

**Example 3** - The following example shows how to display the keywords using the help character '?' (as defined by the \#macro keywords command above) and then run the macro on the port. The \#macro keywords command entered in the macro definition enables the user to receive help for the macro, as shown after the words e.g. below.

```
switchxxxxxx(config-if)#interface gi1
switchxxxxxx(config-if)#macro apply duplex ?
   WORD <1-32>  Keyword to replace with value e.g. $DUPLEX, $SPEED
   <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX ?
   WORD<1-32>  First parameter value
   <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED ?
   WORD<1-32>  Second parameter value
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED 100
```

**4.2 macro**

Use the macro apply/trace Interface Configuration command to either:

- Apply a macro to an interface without displaying the actions being performed
- Apply a macro to the interface while displaying the actions being performed
Syntax

```
macro {apply | trace} macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter-name3 {value}]
```

Parameters

- **apply**—Apply a macro to the specific interface.
- **trace**—Apply and trace a macro to the specific interface.
- **macro-name**—Name of the macro.
- **parameter-name value**—(Optional) For each parameter defined in the macro, specify its name and value. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameter name in the macro are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

The `macro apply` command hides the commands of the macro from the user while it is being run. The `macro trace` command displays the commands along with any errors which are generated by them as they are executed. This is used to debug the macro and find syntax or configuration errors.

When you run a macro, if a line in it fails because of a syntax or configuration error, the macro continues to apply the remaining commands to the interface.

If you apply a macro that contains parameters in its commands, the command fails if you do not provide the values for the parameters. You can use the `macro apply macro-name` with a '?' to display the help string for the macro keywords (if you have defined these with the `#macro keywords` preprocessor command).

Parameter (keyword) matching is case sensitive. All matching occurrences of the parameter are replaced with the provided value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

When you apply a macro to an interface, the switch automatically generates a macro description command with the macro name. As a result, the macro name is
appended to the macro history of the interface. The **show parser macro** command displays the macro history of an interface.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When a macro is applied to an interface range, it is applied sequentially to each interface within the range. If a macro command fails on one interface, it is nonetheless attempted to be applied and may fail or succeed on the remaining interfaces.

**Examples.**

**Example 1** - The following is an example of a macro being applied to an interface with the trace option.

```
switchxxxxxx(config) # interface gi1/1/2
switchxxxxxx(config-if) # macro trace dup $DUPLEX full $SPEED 100
  Applying command... 'duplex full'
  Applying command... 'speed 100'
```

**Example 2** - The following is an example of a macro being applied without the trace option.

```
switchxxxxxx(config) # interface gi1/1/2
switchxxxxxx(config-if) # macro apply dup $DUPLEX full $SPEED 100
```

**Example 3** - The following is an example of an incorrect macro being applied.

```
switchxxxxxx(config-if)#macro trace dup
Applying command...'duplex full'
Applying command...'speed auto'
% bad parameter value
```

4.3 **macro description**

Use the **macro description** Interface Configuration mode command to append a description, for example, a macro name, to the macro history of an interface. Use the **no** form of this command to clear the macro history of an interface. When the
macro is applied to an interface, the switch automatically generates a macro description command with the macro name. As a result, the name of the macro is appended to the macro history of the interface.

**Syntax**

```
macro description text
no macro description
```

**Parameters**

text—Description text. The text can contain up to 160 characters. The text must be double quoted if it contains multiple words.

**Default Configuration**

The command has no default setting.

**Command Mode**

Interface Configuration mode

**User Guidelines**

When multiple macros are applied on a single interface, the description text is a concatenation of texts from a number of previously-applied macros.

To verify the settings created by this command, run `show parser macro`.

**Example**

```
switchxxxxxx(config)＃interface gi1/1/2
switchxxxxxx(config-if)＃macro apply dup
switchxxxxxx(config-if)＃exit
switchxxxxxx(config)＃interface gi1/1/3
switchxxxxxx(config-if)＃macro apply duplex $DUPLEX full $SPEED 100
switchxxxxxx(config-if)＃macro description dup
switchxxxxxx(config-if)＃macro description duplex
switchxxxxxx(config-if)＃end
switchxxxxxx＃show parser macro description
Global Macro(s):
```
4.4 macro global

Use the `macro global` Global Configuration command to apply a macro to a switch (with or without the trace option).

Syntax

```
macro global [apply | trace] macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter-name3 {value}]
```

Parameters

- **apply**—Apply a macro to the switch.
- **trace**—Apply and trace a macro to the switch.
- **macro-name**—Specify the name of the macro.
- **parameter-name value**—(Optional) Specify the parameter values required for the switch. You can enter up to three parameter-value pairs. Parameter
keyword matching is case sensitive. All matching occurrences of the parameters are replaced with the corresponding value.

**Default Configuration**

The command has no default setting.

**Command Mode**

Global Configuration mode

**User Guidelines**

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

If you apply a macro that contains keywords in its commands, the command fails if you do not specify the proper values for the keywords when you apply the macro. You can use this command with a '?' to display the help string for the macro keywords. You define the keywords in the help string using the preprocessor command `#macro keywords` when you define a macro.

When you apply a macro in Global Configuration mode, the switch automatically generates a global macro description command with the macro name. As a result, the macro name is appended to the global macro history. Use `show parser macro` to display the global macro history.

**Example.**

The following is an example of a macro being defined and then applied to the switch with the trace option.

```
switchxxxxxx(config)#  macro name console-timeout
Enter macro commands one per line. End with the character '@'.
line console
exec-timeout $timeout-interval
@
```

```
switchxxxxxx(config)#  macro global trace console-timeout $timeout-interval 100
```
Applying command... ‘line console’
Applying command... ‘exec-timeout 100’
switchxxxxxx(config)#

4.5  macro global description

Use the macro global description Global Configuration command to enter a
description which is used to indicate which macros have been applied to the
switch. Use the no form of this command to remove the description.

Syntax

macro global description text
no macro global description

Parameters

text—Description text. The text can contain up to 160 characters.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

When multiple global macros are applied to a switch, the global description text is
a concatenation of texts from a number of previously applied macros.

You can verify your settings by entering the show parser macro description
privileged EXEC mode command.

Examples

switchxxxxxx(config)#  macro global description "set console timeout interval"
4.6 show parser macro

Use the `show parser macro` User EXEC mode command to display the parameters for all configured macros or for one macro on the switch.

**Syntax**

```
show parser macro [brief | description [interface interface-id | detailed] | name macro-name]
```

**Parameters**

- **brief**—Display the name of all macros.
- **description [interface interface-id]**—Display the macro descriptions for all interfaces or if an interface is specified, display the macro descriptions for that interface.
- **name macro-name**—Display information about a single macro identified by the macro name.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display description of all macros on present ports. If detailed is not used, only present ports are displayed.

**Command Mode**

User EXEC mode

**Examples**

**Example 1** - This is a partial output example from the `show parser macro` command.

```
switchxxxxx# show parser macro
Total number of macros = 6

Macro name : cisco-global
Macro type : default global
```
# Enable dynamic port error recovery for link state failures

<output truncated>

Macro name: cisco-desktop
Macro type: default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

Example 2 - This is an example of output from the show parser macro name command.

switchxxxxxx# show parser macro standard-switch10
Macro name: standard-switch10
Macro type: customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp

Example 3 - This is an example of output from the show parser macro brief command.

switchxxxxxx# show parser macro brief
default global: cisco-global
default interface: cisco-desktop
default interface: cisco-phone
default interface: cisco-switch
default interface: cisco-router
customizable : snmp

This is an example of output from the `show parser macro description` command.

```
switchxxxxx#  show parser macro description
Global Macro(s): cisco-global
```

**Example 4** - This is an example of output from the `show parser macro description interface` command.

```
switchxxxxx#  show parser macro description interface gi1/1/2
Interface Macro Description
------------------------------------------
gi1/1/2 this is test macro
------------------------------------------
```
RSA and Certificate Commands

Keys and Certificates

The device automatically generates default RSA/DSA keys and certificates at following times:

- When the device is booted following a software upgrade.
- When the device is booted with an empty configuration.
- When user-defined keys/certificates are deleted.

Some commands in this section are used to generate user-defined RSA/DSA keys and certificates that replace the default keys and are used by SSL and SSH server commands. Other commands can be used to import these keys from an external source.

These keys and certificates are stored in the configuration files.

The following table describes when these keys/certificates are displayed.

<table>
<thead>
<tr>
<th>File Type Being Displayed</th>
<th>What is Displayed in a Show Command Without Detailed</th>
<th>What is Displayed in a Show Command With Detailed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config</td>
<td>Only user-defined keys/certificates.</td>
<td>Option is not supported.</td>
</tr>
<tr>
<td>Running Config</td>
<td>Keys are not displayed.</td>
<td>All keys (default and user-defined)</td>
</tr>
<tr>
<td>Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)</td>
<td>Keys are displayed as they were copied. There is no distinction here between default and user-defined keys.</td>
<td>Option is not supported.</td>
</tr>
</tbody>
</table>
The following table describes how keys/certificates can be copied from one type of configuration file to another (using the copy command).

<table>
<thead>
<tr>
<th>Destination File Type</th>
<th>Copy from Running Config.</th>
<th>Copy from Startup Config.</th>
<th>Copy from Remote/Local Backup Config. File or Mirror Config. File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config.</td>
<td>All keys/certificates are copied (but only user-defined ones can be displayed)</td>
<td>Option is not supported.</td>
<td>All keys/certificates present in this file are copied.¹²</td>
</tr>
<tr>
<td>Running Config</td>
<td>N/A</td>
<td>Only user defined.</td>
<td>All keys/certificates present in this file are copied.²</td>
</tr>
<tr>
<td>Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)</td>
<td>All keys (default and user)</td>
<td>Only user defined.</td>
<td>All keys/certificates present in this file are copied.²</td>
</tr>
</tbody>
</table>

1. If the Running Configuration file on the device contains default keys (not user-defined ones), the same default keys remain after reboot.

2. In a text-based configuration file, there is no distinction between automatically-defined, default keys and user-defined keys.

### 5.1 crypto key generate dsa

The crypto key generate dsa Global Configuration mode command generates a public and private DSA key (DSA key pair).

**Syntax**

crypto key generate dsa
Parameters
N/A

Default Configuration
The application creates a default key automatically.

Command Mode
Global Configuration mode

User Guidelines
DSA keys are generated in pairs - one public DSA key and one private DSA key.
If the device already has DSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.
Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.
This command is not saved in the Running configuration file. However, the keys generated by this command are saved in a private configuration (which is never displayed to the user or backed up to another device).
See Keys and Certificates for information on how to display and copy this key pair.

Example
The following example generates a DSA key pair.

```
switchxxxxxx(config)# crypto key generate dsa
The SSH service is generating a private DSA key.
This may take a few minutes, depending on the key size.
........
```

5.2 crypto key generate rsa
The crypto key generate rsa Global Configuration mode command generates RSA key pairs.

Syntax
crypto key generate rsa
Parameters
N/A

Default Configuration
The application creates a default key automatically.

Command Mode
Global Configuration mode

User Guidelines
RSA keys are generated in pairs - one public RSA key and one private RSA key. If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

See Keys and Certificates for information on how to display and copy this key pair.

Example
The following example generates RSA key pairs where a RSA key already exists.

```
switchxxxxxx(config)# crypto key generate rsa
Replace Existing RSA Key [y/n]? N
switchxxxxxx(config)#
```

5.3 crypto key import

The crypto key import Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

- `crypto key import {dsa | rsa}`
- `encrypted crypto key import {dsa | rsa}`
- `no crypto key {dsa | rsa}`
RSA and Certificate Commands

Parameters
N/A

Default Configuration
DSA and RSA key pairs do not exist.

Command Mode
Global Configuration mode

User Guidelines
DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

If the device already has DSA/RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is saved in the Running Configuration file.

When using the encrypted key-word, the private key is imported in its encrypted form.

Example

Import an encrypted key

encrypted crypto key import rsa

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key

84et9C2XUfcRlpenuGINAygnLwfkKJcDM6m2ORReALKScqqlhi0wMSSYN1T1WF2P1kEVHH
FptaECZi7HfGlcplpMWzjn1+HaXBTqjPDIEtbpScXqrg6ml1/OEnwpFK2TrmUy01lfkwk8
E/mMfX3i/2rRZLkEBea5jrA6Q62q15naRw1ZkOges+GNeibtvZYSk1jzr56Lur6fT7Xux5i
KMcU2b2Nsud5yW8R/xOCW2e1qDDz/biA2gSgd6FfnW2HV48bTC55eCRsId2MmjbeExUdz
+QRhzcGMBYp6HzdZ6sz8EmSwO+hKd7MIK9U4Sr+Pr1vyWUJ1Ekogz906a2oIgp4tgm4
VDy/K/sI5nVL0+bR81FUXUO/U5hohBcyRUFQ2fHYKZrhT1PT5Rw+PHt6/+EXKG9E+TRs
1UADM1tCRvs+1sB331BdvoR5ld198YaA2ht2ay1Tk6MqCUBdf10+74U0qa/b+bp67wCYKe9
yen418MaYktecHBqM7suU2QUIP34VpmOMyZzc68S/2oT77cy9ihRZx9wcI1yYhJnDiyXP
dgXHxh6kCtcTj6LrUSQuxCJ9su892IWNn50wdgonLSpvfnabv2GHmmelaveL7JJ/7Ucf0
5.4 show crypto key

The `show crypto key` Privileged EXEC mode command displays the device's SSH private and public keys for both default and user-defined keys.

**Syntax**

```
show crypto key [mypubkey] [rsa | dsa]
```

**Parameters**

- `mypubkey`—Displays only the public key.
- `rsa`—Displays the RSA key.
- `dsa`—Displays the DSA key.

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode
User Guidelines

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example displays the SSH public DSA keys on the device.

```
switchxxxxxx# show crypto key mypubkey dsa

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIAwAAAIEAzN31fu56KSE0ZdrGVPIJHpAs8G8NDIkB
dq22qQPiKChLPw0Xsk9tTVkHaZQ5jiBxXn81Q2polaPLJIIH3B1cc96D7IFf
VkbPhMRbz24dpWmPVVLUIQy5nCKdDCui5KVD6zj3gpuhLhMJor7AjAAu5e
BrIi2IuwMVJuakSM098=
---- END SSH2 PUBLIC KEY ----
```

5.5 crypto certificate generate

The crypto certificate generate Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax

```
crypto certificate number generate [key-generate [length]] [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days]
```

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **key-generate length**—Regenerates SSL RSA key and specifies the SSL's RSA key length. (Range: 512–2048)

The following elements can be associated with the key. When the key is displayed, they are also displayed.
- **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters) If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).

- **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)

- **or organization**—Specifies the organization name. (Length: 1–64 characters)

- **loc location**—Specifies the location or city name. (Length: 1–64 characters)

- **st state**—Specifies the state or province name. (Length: 1–64 characters)

- **cu country**—Specifies the country name. (Length: 2 characters)

- **duration days**—Specifies the number of days a certification is valid. (Range: 30–3650)

**Default Configuration**

The default SSL’s RSA key length is 1024.

If **cn common-name** is not specified, it defaults to the device’s lowest static IPv6 address (when the certificate is generated), or to the device’s lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If **duration days** is not specified, it defaults to 365 days.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the RSA key does not exist, you must use the parameter **key-generate**.

If both certificates 1 and 2 have been generated, use **ip https certificate** to activate one of them.

See **Keys and Certificates** for information on how to display and copy this key pair.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.
Example

The following example generates a self-signed certificate for HTTPS whose length is 2048 bytes.

```
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

5.6 crypto certificate request

The `crypto certificate request` Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax

```
crypto certificate number request [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country]
```

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
  - **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
  - **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
  - **or organization**—Specifies the organization name. (Length: 1–64 characters)
  - **loc location**—Specifies the location or city name. (Length: 1–64 characters)
  - **st state**—Specifies the state or province name. (Length: 1–64 characters)
  - **cu country**—Specifies the country name. (Length: 2 characters)

Default Configuration

If `cn common-name` is not specified, it defaults to the device’s lowest static IPv6 address (when the certificate is generated), or to the device’s lowest static IPv4
address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the `crypto certificate generate` Global Configuration mode command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the `crypto certificate import` Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

**Example**

The following example displays the certificate request for HTTPS.

```
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXCzAJBgNVBAgTAmxkMDMwDgYDVQQK
EyMxMjEwMDYwNzE4NjAwMB0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVdP6P0n
WQr0+f+cR5uQ0578f30565jxWi/1wW8ZkK1WY0v2UWwHkCtU8wexBv9q5yH
-----END CERTIFICATE REQUEST-----
```
5.7 crypto certificate import

The `crypto certificate import` Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the RSA key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

Syntax

```
crypto certificate number import
encrypted crypto certificate number import
no crypto certificate number
```

Parameters

- `number`—Specifies the certificate number. (Range: 1–2)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the `crypto certificate request` privileged EXEC command.

If only the certificate is imported, and the public key found in the certificate does not match the device's SSL RSA key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported RSA key, the command fails.

This command is saved in the Running configuration file.

When using the encrypted form of the command, only the private key must be in encrypted format.

See [Keys and Certificates](#) for information on how to display and copy this key pair.
Examples

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

switchxxxxxx(config)# crypto certificate 1 import

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUNQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEMVMBGAUEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XMIAxfOiqlJQJHd4xP+BGHZWwfkJkJUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPlks0L/halpYxp7EWA5t5iDBzSw5s04l0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQAB0AAwDQYJKoZIhvcNAQEEBQAdgYEAuqYiNJst6hI
XFDex7I8od3Uy73dm7FE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s50x7
 Klft/IcjzbBYXLvh45ASWG3TRv2WVKyWs89rPFXu5hXggEeTvWqpuS+gXrIjqW
WVZd0nlFhMacoflgnnEmweIzmrqXBs=
.
-----END CERTIFICATE-----

Certificate imported successfully.

Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 12789788 BB789788

Example 2: The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

switchxxxxxx(config)# crypto certificate 1 import

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

-----BEGIN RSA PRIVATE KEY-----
RSA and Certificate Commands

ACnrqImEGlXkwxBuZU1A09hG91GJsnkf7/MauGFVqxt5vfDf77uQ5CPF49JWQu07cVXh
20wBrHjg6Bv9ULJuuj9p11XPFmX8k8q3N5S7J1InYAWJhJKkbE2MMsKAAA+t/+UzXevvKK6H
TGB67vMxi+hv1LB9zygvq6/+6QfqA51c4nP/8a6Nj0j/ZAQvXNAMKNR2a+eGUooAqLb/C
1l1eqp3Cq5m7+VOPhPSO4dU+NwLvlYCbl1Fb7MFOaA0Nt+2NwGoP0px0vDA9ENLY1ogzS
MlImCmXu52/1xvCE86WFXEBkA+4V81Xqga7KEET657xS7myTJFLJyVawQXNkIU6suTzhhW
2kWNc0/e/vvmpGtlLwxyWynna0fAJF+PawOAdsK75bo79NBim3HcNVhXWznqf2s3AYCRBx
WuGoazpxhZ0s4+7swmM2tS0x14ek43d7RacedGKljPqLHuxXHUn7x215CUpF3abhl+XI
B3u4EECengEvemy9D50snFos+jd5iHrvzEaRAIKfbHa34alVJaNH+2AMC0bhpI3IKreyo
A8Lk6UM0uIqAmnhYf+RyPyXhPQos01pIPHPKBTI6p39XWvicyGRxVspn5+eIYPhe5jYaEn
Ue0nV2RhxNCVnruJAYXSLhjAp5iIqrlJjB/mVt8+zpqcCU9HCWQqsMrNFOFrspcbHu5V4
2Xjmd9tTJ2mhekQqfdwU2bFYKrYsK70ps8u7BtgpRFSRUR7g0lfzhsMuswOBsN6B6pkC
q17y2nBeRS0zrUDgHLLRfwzjwmxjmobXbfYrGMLP4=
------END RSA PRIVATE KEY------
------BEGIN RSA PUBLIC KEY------
MIGHAoGBAMVuFgfJYLbUzmbm6UcLD3ewHYd12MXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4Q85InhgAobBKC96VRSue2rzcoNG4QDkJ2L9ukQ0voFBYNnbzc7a7+7043fwVM+QOXF
TbnRdH1MVrZJGbzzc19zIgky112Xmicy0/nwsXDAgEj
------END RSA PUBLIC KEY------
------BEGIN CERTIFICATE------
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBwMB
IDEVMBMGA1UEAxMNMpAuNS4yMz0uMjJ5MQowCAYDVQQDEwEgMQowCAYDVQQELEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DM3rY
OOg9XM1AxqOiLqLQJHd4xP+F+BHG2WvlfkxKjUDDBz52LxQdU1KrpB/h0+7TFQ0Fv38
7mIDgtnoF1NLsWxkVKRM5LPka0l/halpYxp7EWA51iDBzSw5a041v0bSN7oaGFA
6t4SW2rrnDy8JwWwJWQ1IAABoAawDWYJKoZIhvcNAQEEBQADgYEaBQ1NJst6Hi
XFDxe7I8od3Uyt3Dm7ke/AmuUVOpif2yUly/RuxRKhDp/1Grk12tzLQz5s0ox7
Klf/Icjz8BYXLvh45ASWG3TRv2WVKyWs89rPPXu5hKggEteWwqpuS+gXrIqjW
WVZd0n1fXhMacofignnEmwe1zmrqXb=
------END CERTIFICATE------
.
Certificate imported successfully.
Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788

Example 3 - Import certificate with encrypted key
RSA and Certificate Commands

-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkJT5C+sF0eSyTnxSsfssNo9CoHJ6X9J9lSuktjXU49kaUbTjoQVQatZ
AdQwqWM5mnjUHaJ1M3j9frApY7HaBL3jSxS9jDVrf++/KKhVH6Pxl6vCkVYYzHg43Unm
CNI2n5zf9oisMHU06ugSDs4swVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb71PePefa6
GD/crN28vTLGF/NpyKoOdhAMRuweEoapMo0Py2Cyv+sQLiV42Kck1FPsVFV7X7sh+zVa3
We84pmzyGlY9801PdBSGrJ2xDNCqTvyUpffFEJYJyrdGKYbqD0o3tD/ioUQ3UJgxBGyw
aLLoavSjYY1WkdPjcbn5MVtU5IapCQJXWv3MYC8Q4H3Da6U6N6acUBa1UhgjT+REwWO
DXpJmvx4T/u5W4DPvELqTHyETxgQKNE1079ri2yyLcybUokh+SP+XuxrgG4IKkn8HyKhtz
XeoDojS6e0YQQw2R0nAqz2sZPrgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkpFNkVvFMcidadE+Rwc0m3lKBLcEpNXpFEE3vImsCeyN1pP6eSjQXCCbx2VnmInutyP
CZM927oxkbb41g+U50vQxGhMK7OezTmsf1FdLCmvqV0DHZNR41t4KgqcSjwpQeYszB+4FW
Qmy4tfF4qVdvCly+W1vEpijWpbrCnX9I3RwucNekrm9uf5Zuhd1FA9w8xSWRjWuAq9q
zZFRmDHPhTey9AL02alwpjHOpbJkCMdjHT94ugkF30eyeni9sGN6Y083IvUKby9nBwsA
J0sxrvt3q6cKwKYozQME5LSgxINvQTH48hPtuUz+LNgYw3V5S18DkRejQBM9eaCyjsvLF
+yAI5xA2BDTPqz017FNmhIrXvCqCCXXC+JbgP1PwYTDyD+mnh5v8yV6ST3y7FSC9+5/Sn
Vf8jptLTMWFgFp9Uq9ba8HA7K42XER3R5Zrd0oeUrXQkuRXLhkiufD7HrE7udOmT1F9
W3PqtJ2btjjvMjm5/C+hCo60LNP6q0TEn78EdfaHpmutmMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAM0cA+oB+9ThTgrZeWjdz555FoWwV8s54k5VpuRtvlve5rlzP7ksIL6mvCCXk6J9c
kkr+TsfX63b9t5RgwpGpW8eDHw3q5qkaqInzZh7j2+A+tmxScHulBhpFNY/gmEhGiQf9p
puukcnoTvBNvz73V0vx6h1UHMT0eO+QSeb7xWVAqMBAE=
-----END RSA PUBLIC KEY-----

-----BEGIN CERTIFICATE-----
MIICHCCAYUCEFCCcJ4/dhLsUth10XwObBzngMwDQYJKoZIhvMAQEEBQAwTzEELMAkG
A1UEBhMCICAxCjAIbgNVdAgTASAxCjAIbgNVBAcTASAxEDAogNVBAoMTBzAuMC4w
LjAxCjAIbgNVAbATASAxCjAIbgNVBAsTASAxHhCNNTxM1xMT11d2ZWhcNMTMw
NTIxMT1xN2EzWjBMQswCQYDVQQGEwIEc1EUeMBIBEkMAgGHECMBIBMIDAQgA1UEEw
IDEQMQA4GA1UEAxMMcGMZG4wLjA0MEKMAgGHECMBIBMIDAQgA1UEChMBIBMIDCzAN
BkgkhkG9w0BAQEEFABAoBJwQgYkCqYEAygJor5v2FOCvMR5a3N3JacWbBbXyzniT1

RSA and Certificate Commands

Example 3 - Import certificate with encrypted key

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFktT15c+SFOesSyTnxSssnsNc9CoHj6X9JglSsuktJXU49kauBtjoQVQatZ
AdQwqWM5mnjUhUaJ1MM3WfrApY7aBaL31SxS9jDVrf++/Q/KKhVH6Pxlv6cKvYyZHzg43Unm
CNI2n5zf9oisMH0U6gsIDSySVD1zNgoVQWd7RqKpL9wo3+YVFVS6XCB7pDb71PePef6a6
GD/crN28vTLGf/NpyKoOhdAMRuweQoapMo0Py2Cyv+sqLtv4ZKck1FP1saVFV7X7aH+zVa3
We84pmzyjGiY9S0tpdBSGhJ2xDNcqTYvUpffFEJYrdGKybqD0o3tZ/idUQ3UJgxBGByw
alLoavSjMYiWkdpjfcbn5MVrdu51ApiCQXwv3MYC8GQ4HDa6UDN6aoUB1UhqjT+RExWO
DXpJnvmX4T/u5W4DpELqTHyETxgQKNEr107qRi2yyLcybUohk+SP+XuRkG4IKnn8KyHtz
XeoDjoJS6OYOQw2R0nAqn2zZPgrDzj0zTDL8qvkyurfw4jWa4cvtSclhDEFTHH7NdDLjQ
FkPFNAKvFMcYmidapG+Rwcm031KBLcEpNXpFEE3v1mCeyN1pPe6eSqqMcBxA2vBmInutuP
CZM927oxkb41g+U50yXQgHMK7OeZtmfS1FdlOMfqv0DHZN4R1t4KqgscJjSWPqeYSzb4PW
Qomy4TF4qDvdCLy/WlVepJwpbrdCNXs13RwucNekrm9uf5Zubd1FA9wf8XswRJwUaqgq
zZFRmDMHPTey9AL02alpwjH0PbJKiCMdjHT94ugkF30eyeni9sGN6Y0363vUkKy6nbwasa
J0sxrvt3q6cblkLoZymQ65LsLQnxQlH4BhPtu+LUNqWb3V5S18DkKrejQB99eaCyJsvLF
+yAI5xABZdTPqz017FNNzhIrXvCqCCcx+JbgP1FwYDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
-----END CERTIFICATE-----
```

Certificate imported successfully.

Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU= 
Valid From: Jan 24 18:41:24 2011 GMT 
Valid to: Jan 24 18:41:24 2012 GMT 
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU= 

SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
Certificate imported successfully.

Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=

Valid From: Jan 24 18:41:24 2011 GMT

Valid to: Jan 24 18:41:24 2012 GMT

Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=

SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
5.8 show crypto certificate

The `show crypto certificate` Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

**Syntax**

```
show crypto certificate [mycertificate] [number]
```

**Parameters**

- `number`—Specifies the certificate number. (Range: 1,2)
- `mycertificate`—Specifies that only the certificate will be displayed

**Default Configuration**

Certificate number 1.

**Command Mode**

Privileged EXEC mode

**Examples**

**Example 1** - The following example displays SSL certificate # 1 present on the device.

```
switchxxxxxx# show crypto certificate mycertificate
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAAQLADBIAkEAp4HShnnH/xQSGA2ffkRBwU2IXb7n8VFsTm1xyJlt1la1GaqchfMqge0kmfhcoHSWr
ynf1PDPWMOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDagFQMA8GA1UdEBEB/wQFMAMBAf8wHgYDVVR0OBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVRF0fBIBLTCCASkwqKogcc+ggcyGgcsZGFwOi8v
L0VByb3h5JT1wU29mdHdhcmUlmJBSb290JT1wQ2VydGlmaWVyLENOPXNlc3Nl
-----END CERTIFICATE-----
Issued by: www.verisign.com
```
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Fingerprint: DC789788 DC88A988 127897BC BB789788

Certificate 2:
Certificate Source: User-Defined

-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWzpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HSnnH/xQSGA2ffkRBwU2XIx7n8VFSTmlxyJ1t11a1GaqchfMqqe0kmfhcoHSwrz
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAAEw
CwR0PBAQDAgFGMA8GA1dgEEXR0fBIIBLTCCASkgJggc+ggcyGgc1sZGFwOi8v
L0VByb3h5JTIwU29mdHcmlhUkMBSb290JTIwQ2VydGlmaWVyLENOPX1cnZl

-----END CERTIFICATE-----
Issued by: www.verisign.com
Valid from: 8/9/2004 to 8/9/2005
Subject: CN= router.gm.com, O= General Motors, C= US
Fingerprint: DC789788 DC88A988 127897BC BB789788

Example 2

The following example displays SSL certificate #1 present on the device and the key-pair.

```
switchxxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default

-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWzpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HSnnH/xQSGA2ffkJRBwU2XIx7n8VFSTmlxyJ1t11a1GaqchfMqqe0kmfhcoHSwrz
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAAEw
CwR0PBAQDAgFGMA8GA1dgEEXR0fBIIBLTCCASkgJggc+ggcyGgc1sZGFwOi8v
L0VByb3h5JTIwU29mdHcmlhUkMBSb290JTIwQ2VydGlmaWVyLENOPX1cnZl

-----END CERTIFICATE-----
```
RSA and Certificate Commands

-----BEGIN CERTIFICATE-----
L0VByb3h5JTJwU29mdHdhcmU1MTI5O3h5c2VydGlmaWVyLENOPXN1cnZl
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
ACnrqImEG1xkwBuEULAO9nHg9IGJsnkf7/MauGPVq5cStq77uQSCPf49JWWhu07cVXh
20wrBlGJbB69vLUlJujm9pl1XpMk9qR3NS7JZ1InYAWHKhKbE7MmKSA6+t/uzVxevKK6H
TGB7wMxh+lvBL9zygyVq6/+6Qfqa51ic4nF/8a6Nj0/ZOAvgNAMKNrZ2Wz+tuGUoaQgL0b/C
11eEqzpcQ5mT7+U0kHPSO4dUU+Nwlv1YcBlFB7MFOaON+y+2NwoGp0pxOvDA9ENY17qsZ
MiwmCfxU52/IxC7fD8FWxEBtk4vV81Xqa7K6ET657xS7m8yTJFLZ2yVawGJXh1Us6uTzhhW
DKWwC0e/vwMgPtl1WyxyWynnaPoFAJ+FawOAdsk75bo79NBxm3HcNVxWzNqzfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RacedGKljhpLHzUXHUon7Zx15CUtP3shH+XI
B3u4EEcEngYMewy5obn1vnFSct+d5JHuzRzEuARIsFhHa34a1VJaN+2AMCB0hp13IkreYo
A8lK6UMOuIqAnhYf+RyFXhPOQs01PpIPKHBGTi6pqj39XMv1yRXvSpn5+eIYPhve5jYaEn
UeOnVZrhNCvnuJAYXSLhjApf5iIqr1JiJb/mvT8+ZpqCUC9HCWQqSnrNFOFrSpceHu5V4
ZX4jmd9tTJZmhekoQflbdwU2bfYkRYSk70ps8u87BgtgRf5SRU7g0LzfzhMusw0DsnB65pkC
q17yZnBeRS0zrUDgHLLRfzwjwmxjmwObxyYfRGMlp4=
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MI8H0aGBAVMVaFgjJlyUnzmbm6ucLD3ewHYd12MXY4A3KLFL2SUXudlTIq84aME8DIiSFB2
Cqy4Q5InhaoAbIBK96VRseUerzoNG4QDkj2L9uktQOovFBNmbzHc7a+7043wFVmh+QOFf
TbnRoHlmVrZJGbx11c9iZgkly121Xmicy0/nwsXDAgEj
-----END RSA PUBLIC KEY-----

Issued by: www.verisign.com

Valid from: 8/9/2003 to 8/9/2004

Subject: CN= router.gm.com, 0= General Motors, C= US

Fingerprint: DC789788 DC88A988 127897BC BB789788
6.1 ping

Use the ping EXEC mode command to send ICMP echo request packets to another node on the network.

Syntax

```
ping [ip] [ipv4-address | hostname] [size packet_size] [count packet_count] [timeout time_out] [source source-address]
ping ipv6 [ipv6-address | hostname] [size packet_size] [count packet_count] [timeout time_out] [source source-address]
```

Parameters

- **ip**—Use IPv4 to check the network connectivity.
- **ipv6**—Use IPv6 to check the network connectivity.
- **ipv4-address**—IPv4 address to ping.
- **ipv6-address**—Unicast or Multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. See IPv6z Address Conventions.
- **hostname**—Hostname to ping (Length: 1-160 characters. Maximum label size for each part of the host name: 58.)
- **size packet_size**—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4: 64–1518, IPv6: 68–1518)
- **count packet_count**—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- **time time-out**—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).
- **source source-address**—Source address (Unicast IPv4 address or global Unicast IPv6 address).
Default Usage
N/A

Command Mode
EXEC mode

User Guidelines
Press Esc to stop pinging. Following are sample results of the ping command:

- **Destination does not respond**—If the host does not respond, a “no answer from host” appears within 10 seconds.
- **Destination unreachable**—The gateway for this destination indicates that the destination is unreachable.
- **Network or host unreachable**—The switch found no corresponding entry in the route table.

See IPv6z Address Conventions.

When using the ping **ipv6** command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the IPv6Z format. If the egress interface is not specified, the default interface is selected.

When using the ping **ipv6** command with a Multicast address, the information displayed is taken from all received echo responses.

When the **source** keyword is configured and the source address is not an address of the switch, the command is halted with an error message and pings are not sent.

Examples

**Example 1 - Ping an IP address.**

```
switchxxxxxx# ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```
Example 2 - Ping a site.
switchxxxxxx# ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Example 3 - Ping an IPv6 address.
switchxxxxxx# ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50

switchxxxxxx# ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::33: icmp_seq=1. time=70 ms
64 bytes from 3003::11: icmp_seq=2. time=0 ms
6.2 traceroute

To display the routes that packets will take when traveling to their destination, use the `traceroute` EXEC mode command.

Syntax

```
traceroute ip [ipv4-address | hostname] [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
traceroute ipv6 {ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```

Parameters

- `ip`—Use IPv4 to discover the route.
- `ipv6`—Use IPv6 to discover the route.
- `ipv4-address`—IPv4 address of the destination host.
- `ipv6-address`—IPv6 address of the destination host.
- `hostname`—Hostname of the destination host. (Length: 1-160 characters. Maximum label size for each part of the host name: 58.)
- `size packet_size`—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- `ttl max-ttl`—The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached. (Range: 1–255)

- `count packet_count`—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)

- `timeout time_out`—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)

- `source ip-address`—One of the interface addresses of the device to use as a source address for the probes. The device selects the optimal source address by default. (Range: Valid IP address)

- `tos tos`—The Type-Of-Service byte in the IP Header of the packet. (Range: 0–255)

**Default Usage**

N/A

**Command Mode**

EXEC mode

**User Guidelines**

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute command is not relevant to IPv6 link local addresses.
Example

```
switchxxxxxxx# traceroute ip umaxpl.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxpl.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45 msec
7 so-0-2-0x1.aal.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec 58 msec
11 umaxpl.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63 msec
```

Trace completed

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the router in the path to the host.</td>
</tr>
<tr>
<td>i2-gateway.stanford.edu</td>
<td>Host name of this router.</td>
</tr>
<tr>
<td>192.68.191.83</td>
<td>IP address of this router.</td>
</tr>
<tr>
<td>1 msec 1 msec 1 msec</td>
<td>Round-trip time for each of the probes that are sent.</td>
</tr>
</tbody>
</table>

The following are characters that can appear in the traceroute command output:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.</td>
</tr>
</tbody>
</table>
6.3 telnet

The `telnet` EXEC mode command logs on to a host that supports Telnet.

**Syntax**

```
telnet {ip-address | hostname} [port] [keyword...]
```

**Parameters**

- `ip-address`—Specifies the destination host IP address (IPv4 or IPv6).
- `hostname`—Specifies the destination host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 58.)
- `port`—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- `keyword`—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

**Default Configuration**

The default port is the Telnet port (23) on the host.

**Command Mode**

EXEC mode

**User Guidelines**

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating
system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

**Special Telnet Sequences**

<table>
<thead>
<tr>
<th>Telnet Sequence</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-shift-6-b</td>
<td>Break</td>
</tr>
<tr>
<td>Ctrl-shift-6-c</td>
<td>Interrupt Process (IP)</td>
</tr>
<tr>
<td>Ctrl-shift-6-h</td>
<td>Erase Character (EC)</td>
</tr>
<tr>
<td>Ctrl-shift-6-o</td>
<td>Abort Output (AO)</td>
</tr>
<tr>
<td>Ctrl-shift-6-t</td>
<td>Are You There? (AYT)</td>
</tr>
<tr>
<td>Ctrl-shift-6-u</td>
<td>Erase Line (EL)</td>
</tr>
</tbody>
</table>

At any time during an active Telnet session, available Telnet commands can be listed by pressing the `?/help` keys at the system prompt.

A sample of this list follows.

```
switchxxxxxx# ?/help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
?/help suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.
### Keywords Table

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/echo</td>
<td>Enables local echo.</td>
</tr>
<tr>
<td>/quiet</td>
<td>Prevents onscreen display of all messages from the software.</td>
</tr>
<tr>
<td>/source-interface</td>
<td>Specifies the source interface.</td>
</tr>
<tr>
<td>/stream</td>
<td>Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.</td>
</tr>
<tr>
<td>Ctrl-shift-6 x</td>
<td>Returns to the System Command Prompt.</td>
</tr>
</tbody>
</table>

### Ports Table

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>179</td>
</tr>
<tr>
<td>chargen</td>
<td>Character generator</td>
<td>19</td>
</tr>
<tr>
<td>cmd</td>
<td>Remote commands</td>
<td>514</td>
</tr>
<tr>
<td>daytime</td>
<td>Daytime</td>
<td>13</td>
</tr>
<tr>
<td>discard</td>
<td>Discard</td>
<td>9</td>
</tr>
<tr>
<td>domain</td>
<td>Domain Name Service</td>
<td>53</td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td>7</td>
</tr>
<tr>
<td>exec</td>
<td>Exec</td>
<td>512</td>
</tr>
<tr>
<td>finger</td>
<td>Finger</td>
<td>79</td>
</tr>
<tr>
<td>ftp</td>
<td>File Transfer Protocol</td>
<td>21</td>
</tr>
<tr>
<td>ftp-data</td>
<td>FTP data connections</td>
<td>20</td>
</tr>
<tr>
<td>gopher</td>
<td>Gopher</td>
<td>70</td>
</tr>
<tr>
<td>hostname</td>
<td>NIC hostname server</td>
<td>101</td>
</tr>
<tr>
<td>ident</td>
<td>Ident Protocol</td>
<td>113</td>
</tr>
<tr>
<td>irc</td>
<td>Internet Relay Chat</td>
<td>194</td>
</tr>
<tr>
<td>klogin</td>
<td>Kerberos login</td>
<td>543</td>
</tr>
<tr>
<td>kshell</td>
<td>Kerberos shell</td>
<td>544</td>
</tr>
<tr>
<td>login</td>
<td>Login</td>
<td>513</td>
</tr>
<tr>
<td>lpd</td>
<td>Printer service</td>
<td>515</td>
</tr>
</tbody>
</table>
## System Management Commands

### 6.4 resume

The `resume` EXEC mode command enables switching to another open Telnet session.

**Syntax**

`resume [connection]`

**Parameters**

`connection`—Specifies the connection number. (Range: 1-4 connections.)

---

**Example**

The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
switchxxxxxx# telnet 176.213.10.50
```

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>nntp</td>
<td>Network News Transport Protocol</td>
<td>119</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>PIM Auto-RP</td>
<td>496</td>
</tr>
<tr>
<td>pop2</td>
<td>Post Office Protocol v2</td>
<td>109</td>
</tr>
<tr>
<td>pop3</td>
<td>Post Office Protocol v3</td>
<td>110</td>
</tr>
<tr>
<td>smtp</td>
<td>Simple Mail Transport Protocol</td>
<td>25</td>
</tr>
<tr>
<td>sunrpc</td>
<td>Sun Remote Procedure Call</td>
<td>111</td>
</tr>
<tr>
<td>syslog</td>
<td>Syslog</td>
<td>514</td>
</tr>
<tr>
<td>tacacs</td>
<td>TAC Access Control System</td>
<td>49</td>
</tr>
<tr>
<td>talk</td>
<td>Talk</td>
<td>517</td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet</td>
<td>23</td>
</tr>
<tr>
<td>time</td>
<td>Time</td>
<td>37</td>
</tr>
<tr>
<td>uucp</td>
<td>Unix-to-Unix Copy Program</td>
<td>540</td>
</tr>
<tr>
<td>whois</td>
<td>Nickname</td>
<td>43</td>
</tr>
<tr>
<td>www</td>
<td>World Wide Web</td>
<td>80</td>
</tr>
</tbody>
</table>
Default Configuration
The default connection number is that of the most recent connection.

Command Mode
EXEC mode

Example
The following command switches to open Telnet session number 1.

```
switchxxxxxx# resume 1
```

6.5 hostname

The `hostname` Global Configuration mode command specifies or modifies the device host name. Use the no form of the command to remove the existing host name.

Syntax

```
hostname name
no hostname
```

Parameters

**Name**—Specifies the device host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 58). The hostname must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

Default Configuration
No host name is defined.

Command Mode
Global Configuration mode

Example
The following example specifies the device host name as ‘enterprise’.
switchxxxxxx(config)# hostname enterprise
enterprise(config)#

6.6 reload

The reload Privileged EXEC mode command reloads the operating system at a user-specified time.

Syntax

reload [[in [hhh:mm | mmm] | at hh:mm [day month]] | cancel] [slot unit-id]

Parameters

- **in hhh:mm | mmm** - Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.

- **at hh:mm** - Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

- **day** - Number of the day in the range from 1 to 31.

- **month** - Month of the year.

- **cancel** - Cancels a scheduled reload.

- **slot unit-id**—Specifies the unit number to be reloaded. (Range: 1–8). If unspecified, reloads all the units.

Default Usage

N/A

Command Mode

Privileged EXEC mode
User Guidelines

The `at` keyword can be used only if the system clock has been set on the device. To schedule reloads across several devices to occur simultaneously, synchronize the time on each device with SNTP.

When you specify the reload time using the `at` keyword, if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

To display information about a scheduled reload, use the `show reload` command.

Examples

**Example 1:** The following example reloads the operating system on all units of a stack system or on the single unit of a standalone system.

```
switchxxxxxx# reload
This command will reset the whole system and disconnect your current session.
Do you want to continue? (y/n) [Y]
```

**Example 2:** The following example reloads the operating system in 10 minutes on all on all units of a stack system or on the single unit of a standalone system.

```
switchxxxxxx# reload in 10
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you want to continue? (y/n) [Y]
```

**Example 3:** The following example reloads the operating system at 13:00 on all on all units of a stack system or on the single unit of a standalone system.

```
switchxxxxxx# reload at 13:00
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes). Do you want to continue? (y/n) [Y]
```
Example 4: The following example cancels a reload.

```
switchxxxxxx# reload cancel
Reload cancelled.
```

6.7 show reload

The `show reload` Privileged EXEC mode command displays whether there is a pending reload for status of the device.

Syntax

```
show reload
```

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

You can use this command to display a pending software reload. To cancel a pending reload, use this command with the `cancel` parameter.

Example

The following example displays that reboot is scheduled for 00:00 on Saturday, April-20.

```
switchxxxxxx# show reload
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```
6.8  **service cpu-utilization**

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
service cpu-utilization
no service cpu-utilization
```

**Parameters**

N/A

**Default Configuration**

Measuring CPU utilization is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the **service cpu utilization** command to measure information on CPU utilization.

**Example**

The following example enables measuring CPU utilization.

```
switchxxxxxx(config)# service cpu-utilization
```

---

6.9  **show cpu utilization**

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

**Syntax**

```
show cpu utilization
```

---
### Parameters

N/A

### Default Usage

N/A

### Command Mode

Privileged EXEC mode

### User Guidelines

Use the `show cpu-utilization` command to enable measuring CPU utilization.

### Example

The following example displays CPU utilization information.

```plaintext
switchxxxxxx# show cpu-utilization
CPU utilization service is on.
CPU utilization

----------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

### 6.10 show users

The `show users` EXEC mode command displays information about the active users.

#### Syntax

```plaintext
show users
```

#### Parameters

N/A

#### Default Usage

N/A
Command Mode
EXEC mode

Example
The following example displays information about the active users.

```
switchxxxxxx# show users
Username  Protocol  Location
----------  --------  ----------
Bob        Serial   Serial 172.16.0.1
John       SSH      SSH    172.16.0.8
Robert     HTTP     HTTP   172.16.1.7
Betty      Telnet   Telnet 172.16.1.6
Sam        Serial   Serial 172.16.1.6
```

6.11 show sessions
The `show sessions` EXEC mode command displays open Telnet sessions.

Syntax
```
show sessions
```

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

User Guidelines
The `show sessions` command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.
Example

The following example displays open Telnet sessions.

```
switchxxxxxx# show sessions
```

<table>
<thead>
<tr>
<th>Connection</th>
<th>Host</th>
<th>Address</th>
<th>Port</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote router</td>
<td>172.16.1.1</td>
<td>23</td>
<td>89</td>
</tr>
<tr>
<td>2</td>
<td>172.16.1.2</td>
<td>172.16.1.2</td>
<td>23</td>
<td>8</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>The connection number.</td>
</tr>
<tr>
<td>Host</td>
<td>The remote host to which the device is connected through a Telnet session.</td>
</tr>
<tr>
<td>Address</td>
<td>The remote host IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The Telnet TCP port number.</td>
</tr>
<tr>
<td>Byte</td>
<td>The number of unread bytes for the user to see on the connection.</td>
</tr>
</tbody>
</table>

6.12 show system

The `show system` EXEC mode command displays system information.

Syntax

```
show system unit unit-id
```

Parameters

`unit-id`—Specifies the unit number. (Range: 1–8)

Command Mode

EXEC mode
Example

```
switchxxxxxx# show system unit 2
System Description: xxxx
System Up Time (days,hour:min:sec): 08,23:03:46
System Contact:
System Name:
System Location:
System MAC Address: 00:99:88:66:33:33
System Object ID: 1.3.6.1.4.1.674.10895.3031
Main Power Supply Status: OK
#Editor: For systems with a single Fan or single Fans’ status
Fans Status: OK
#Editor: For systems with multiple Fans which support status per Fan
Unit   FAN1      FAN2         FAN3          FAN4         FAN5
---- -------- -----------  ------------ ------------ -------------
2       OK        OK        NOT PRESENT    FAILURE      IDLE
#Editor: For systems with no temperature sensors, the temperature in the
following line will be blank and the Status will be N/A
Unit Temperature (Celsius) Status
---- --------------------- -----
2    42                    OK
```

6.13 show environment

The **show environment** EXEC mode command displays environment information.

**Syntax**

```
show environment {all | fan | temperature {status} | stack [switch-number]}
```
Parameters

- **all**—Displays the fan and temperature general status
- **fan**—Displays the fan status
- **temperature status**—Displays the temperature status
- **stack switch-number**—Displays detailed environment status of a stack. If the switch-number is specified, the environment status of the selected device number is displayed. (Range: 1–8)

Command Mode

EXEC mode

User Guidelines

The **fan** and **temperature status** parameters are available only on devices on which FAN and/or temperature sensor are installed.

Fan status can be one of:

- **OK** - The fan/s functions correctly.
- **Failure** - The fan failed.
- **NA** - No fan is installed.
- **Not Present** - Fan module was removed.

Sensor status can be one of:

- **OK** - The sensor/s functions correctly.
- **Failure** - The sensor/s failed.
- **NA** - No sensor is installed.

Temperature can be one of:

- **OK** - The temperature is below the warning threshold.
- **Warning** - The temperature is between the warning threshold to the critical threshold.
- **Critical** - the temperature is above the critical threshold.

Example

The following example displays the general environment status of a device or a stack.
switchxxxxxxx # show environment all
FAN is OK
TEMPERATURE is OK

The following example displays the general FAN status of a device or a stack.
switchxxxxxxx # show environment fan
FAN is OK

The following example displays the detailed temperature status of a device or a stack.
switchxxxxxxx # show environment temperature status
TEMPERATURE is Warning

The following example displays the detailed environment status of a stack.
switchxxxxxxx # show environment stack

<table>
<thead>
<tr>
<th>Unit</th>
<th>FAN Status</th>
<th>FAN Direction*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OK</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>Failure</td>
<td>Front-to-Back</td>
</tr>
<tr>
<td>3</td>
<td>OK</td>
<td>Back-to-Front</td>
</tr>
<tr>
<td>4</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Not Present</td>
<td></td>
</tr>
</tbody>
</table>

#EDITOR: * FAN Direction column will be printed only in SKUs which support this feature, or in a stack when one of the units might support this feature.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Sensor Status</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>
6.14 show inventory

The show inventory EXEC mode command displays system information.

Syntax

show inventory [entity]

Parameters

entity—Specifies the entity to be displayed. It can be a number (1-8) for a specific unit number, or an interface (Ethernet) name.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays all the entities in a standalone system.

switchxxxxxx # show inventory
NAME: "1", DESCR: "52-Port Gigabit PoE Stackable Managed Switch"
PID: SRW224G4P-K9, VID: V01, SN: 123456789

Example 2 - The following example displays a specific entity in a standalone system.

switchxxxxxx # show inventory gigabitethernet2/1/49
NAME: "GigabitEthernet2/1/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1, VID: V01, SN: AGC1525UR7G

Example 3 - The following example displays all the entities in a stacking system with two units.

switchxxxxxx # show inventory
NAME: "2", DESCR: "52-Port Gigabit PoE Stackable Managed Switch"
PID: SRW224G4P-K9, VID: V01, SN: 123456789
NAME: "GigabitEthernet2/1/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1, VID: V01, SN: AGC1525UR7G
NAME: "4", DESCR: "52-Port Gigabit PoE Stackable Managed Switch"
Example 4 - The following example displays information for unit 1 of the stack.

```
switchxxxxxx # show inventory 1
NAME: "1"  DESCR: "48-Port Gigabit with 4-Port 10-Gigabit PoE Stackable Managed Switch"
PID: SG500X-48P-K9  VID: V02  SN: 402
```

### 6.15 show version

The `show version` EXEC mode command displays system version information.

**Syntax**

```
show version[unit unit-id]
```

**Parameters**

- `unit`—Specifies the unit number. (Range: 1–8)

**Default Usage**

Show version on all units if no unit is specified.

**Command Mode**

EXEC mode

**Example**

The following example displays system version information.

```
switchxxxxxx# show version
SW Version 1.1.0.5 ( date 15-Sep-2010 time 10:31:33 )
Boot Version 1.1.0.2 ( date 04-Sep-2010 time 21:51:53 )
HW Version V01
Unit SW Version Boot Version HW Version
------ ----------- ------------ ----------
1 3.131 2.178 1.0.0
```
### 6.16 show version md5

Use the `show version md5` EXEC mode command to display external MD5 digest of firmware.

**Syntax**

```
show version md5 [unit unit-id]
```

**Parameters**

- `unit unit-id`—Unit number. (Range: 1–8)

**Default Usage**

N/A

**Command Mode**

EXEC mode

**Example**

```
switchxxxxx# show version md5

Unit Filename Status MD5 Digest
----  -------- ------- ----------------------------------
 1     image1 Active 23FA000012857D8855AABC7577AB5562
 1     image2 Not Active 23FA000012857D8855AABEA7451265456
 1     boot 23FA000012857D8855AABC7577AB8999
 2     image1 Not Active 23FA000012857D8855AABC7577FE693844
 2     image2 Active 23FA000012857D8855AABC7577AB5562
 2     boot 23FA000012857D8855AABC7577AC9999
```

### 6.17 set system

The `set system` Privileged EXEC mode command puts the device into various modes depending on the parameters entered.
Syntax

set system mode {router | switch} queues-mode {4|8}

Parameters

- router—Specifies that the device functions as a switch-router.
- switch—Specifies that the device functions as a switch.
- queues-mode {4|8}—Specifies that the system uses 4 or 8 QoS queues.

Default Configuration

The default configuration is switch mode (Layer 2), with 4 QoS queues.

Command Mode

Privileged EXEC mode

User Guidelines

The switch/router parameters are not relevant for SG500X/ESW2-550X Devices in standalone and native mode.

The system mode and the queues mode appears in the configuration file header to specify the system mode. It appears even if it specifies the default system mode.

Changing the system mode (e.g. switch->router):

- Manually setting the system mode: If this command is entered manually, the Startup Configuration file is deleted and the device is rebooted. It is highly recommended to back up the Startup Configuration file before executing this command since the device will be configured in the new system mode with an empty configuration.

- Configuration download: If the system mode is contained in a configuration file that is downloaded to the device, but the system mode in the downloaded file matches the current system mode, this information is ignored. Otherwise the following cases might occur:
  1. If this file is copied manually onto the device (using copy tftp, for example), the operation is aborted, and a message is displayed indicating that the system mode must be changed manually.
  2. If this file is downloaded during the automatic configuration process, the Startup Configuration file is deleted and the device reboots automatically in the new system mode and the device is configured with an empty configuration.
Changing the queues mode (e.g. 4 queues to 8 queues):

Changing the queues mode takes effect after rebooting the system.

- When upgrading the queues mode from 4 queues to 8 queues, the queue-related configurations needs to be examined and adjusted such that it will meet the desired QOS objectives with the new queues mode.

- When downgrading the queues mode from 8 queues to 4 queues, if Queue-related configuration exist on the startup configuration file, the system will reject the downgrade of queues and will require the user to delete all the queue-related configuration from the startup configuration file before downgrading the queues mode. When changing the queues mode during configuration download to startup configuration file, the existing queues configuration is not tested and the download will not be rejected.

Examples

**Example** - The following example configures the device to function as a switch-router (Layer 3), and sets the queues mode to 8 queues.

```
switchxxxxxx# set system mode router queues-mode 8
```

**Example** - The following example tries to configure the device to function as a switch-router (Layer 3), using tftp download, while the device is currently configured to function as a switch (layer 2), therefore the configuration file download will fail.

```
switchxxxxxx# copy tftp://102.1.2.2/file1 startup-config
```

Copy operation aborted, the downloaded configuration file is for Router system mode while the device is currently in switch system mode. Please change the system mode before downloading this file.

**Example** - The following example displays the system mode and the queues mode. In this example the device was configured to function as a switch-router (Layer 3), and the queues mode to 8 queues.

```
switchxxxxxx# show running-configuration
config-file-header
```
6.18 show system mode

The `show system mode` EXEC mode command displays information on features control.

---

**Note**

This chapter is only relevant for Sx500 devices.

**Syntax**

`show system mode`

**Parameters**

N/A

**Default Usage**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays system mode information.
switchxxxxxxx# show system mode

Feature | State
--------|-------
Mode: | Router
Queues Configuration: | 8 Queues
Active

### 6.19 show system languages

The `show system languages` EXEC mode command displays the list of supported languages.

**Syntax**

`show system languages`

**Parameters**

N/A

**Default Usage**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays the languages configured on the device. Number of Sections indicates the number of languages permitted on the device.

```
switchxxxxxxx# show system languages

Language Name | Unicode Name | Code  | Num of Sections
--------------|-------------|-------|-----------------|
English       | English     | en-US | 2
Japanese      | µฉูฉื Fernandez | ja-JP | 2
```
6.20 show system tcam utilization

The **show system tcam utilization** EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

**Syntax**

```plaintext
show system tcam utilization [unit unit-id]
```

**Parameters**

N/A

**Default Usage**

`unit-id`—Specifies the unit number. (Range: 1–8)

**Command Mode**

EXEC mode

**Example**

The following example displays TCAM utilization information.

```
switchxxxxxx# show system tcam utilization
TCAM utilization: 58%
System: 75%
Unit | TCAM utilization [%]
-----|---------------------
    |---------------------
 1   | 58
 2   | 57
```

6.21 show services tcp-udp

Use the **show services tcp-udp** Privileged EXEC mode command to display information about the active TCP and UDP services.

**Syntax**

```plaintext
show services tcp-udp
```
**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

The output does not show sessions where the device is a TCP/UDP client.

**Examples**

```
switchxxxxxx# show services tcp-udp
Type  Local IP Address  Remote IP address  Service Name  State
TCP   All:22            SSH               LISTEN
TCP   All:23            Telnet             LISTEN
TCP   All:80            HTTP              LISTEN
TCP   All:443           HTTPS             LISTEN
TCP   172.16.1.1:23 172.16.1.18:8789  Telnet     ESTABLISHED
TCP6  All-23           Telnet             LISTEN
TCP6  fe80::200:b0ff:fe00:0-23 fe80::200:b0ff:fe00:0-8999 Telnet   ESTABLISHED
UDP   All:161          SNMP               
UDP6A 11-161           SNMP               
```

**6.22 show tech-support**

Use the **show tech-support** EXEC mode command to display system and configuration information that can be provided to the Technical Assistance Center when reporting a problem.

**Syntax**

```
show tech-support [config | memory]
```
Parameters

- memory—Displays memory and processor state data.
- config—Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output of technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

EXEC mode

User Guidelines

Caution: Avoid running multiple show tech-support commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The show tech-support command may time out if the configuration file output takes longer to display than the configured session time out time. If this happens, enter a set logout timeout value of 0 to disable automatic disconnection of idle sessions or enter a longer timeout value.

The show tech-support command output is continuous, meaning that it does not display one screen at a time. To interrupt the output, press Esc.

If the user specifies the memory keyword, the show tech-support command displays the following output:

- Flash info (dir if exists, or flash mapping)
- Output of command show bootvar
- Buffers info (like print os buff)
- Memory info (like print os mem)
- Proc info (like print OS tasks)
- Versions of software components
### 6.23 system recovery

Use the `system recovery` Global Configuration command to set the system to automatically recover from temperature that reached the critical threshold.

Use the `no` form of the command to return to disable automatic recovery.

**Syntax**

```
system recovery
no system recovery
```

**Parameters**

N/A

**Default Configuration**

System recovery is enabled by default.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# no system recovery
```

### 6.24 show system fans

Use the `show system fans` EXEC mode command to view the status of the fans on the device.

**Syntax**

```
show system fans [unit-id]
```
Parameters

unit-id—Specifies the unit number to be reloaded. (Range: 1–8). If unspecified, displays information for all the units.

Default Usage

N/A

Command Mode

EXEC mode

Example

Example 1: If the device does not support controlled fan direction, the column Fan Direction is not displayed.

switchxxxxxx# show system fans
Unit  Oper state  Fan Direction
---  ----------  ----------- --------------
1    on         Back to front
2    fail

Example 2: For devices whose hardware supports variable fan speed.

#Editor: For systems with no support for Fan direction

switchxxxxxx# show system fans
Unit  Speed  Oper state
---  ---------  --------------
1    8000     on
2    8000     on

6.25 show system sensors

Use the show system sensors EXEC mode command to view the temperature sensor status

Syntax

show system sensors
Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

Example

Example 1: For Standalone systems with a single sensor status

```
switchxxxxxx# show system sensors
Sensor Status: OK
Temperature(C): 37
```

---

Example 2: For systems with multiple sensor statuses

```
Sensor  Sensor     Temperature(c)
Status
---    ---------  --------------
1      OK         37
2      Failure
```

---

Example 3: For systems with a single sensor status

```
switchxxxxxx# show system sensors
Unit  Sensor     Temperature(c)
Status
---  ---------  --------------
1    OK         37
2    Failure
3    OK         68
```
**Example 4:** For systems with multiple sensor statuses

<table>
<thead>
<tr>
<th>Unit/ Sensor</th>
<th>Sensor Status</th>
<th>Temperature(c)</th>
<th>Alarm Temp(C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>OK</td>
<td>37</td>
<td>60</td>
</tr>
<tr>
<td>1/2</td>
<td>Failure</td>
<td></td>
<td>60</td>
</tr>
<tr>
<td>2/1</td>
<td>OK</td>
<td>68</td>
<td>65</td>
</tr>
</tbody>
</table>

### 6.26  **show system id**

The *show system id* EXEC mode command displays the system identity information.

**Syntax**

```
show system id [unit unit-id]
```

**Parameters**

*unit unit-id*—Unit number or all. If unspecified, defaults to all. (Range: 1–8)

**Command Mode**

EXEC mode

**Example**

The following example displays the system identity information.

```
switchxxxxxx# show system id
serial number 114disable ports leds
```

Use the *disable ports leds* Global Configuration mode command to turn off the LEDs on all ports on a device.

Use the *no disable ports leds* command to set the LEDs of all the ports on the device to their current operational status of the port.

**Syntax**

```
disable ports leds
```
no disable ports leds

Parameters
N/A

Default Configuration
The default is no disable port leds; that is the LEDs of all the ports reflect their current status.

Command Mode
Global Configuration mode

User Guidelines
N/A

Examples
The following example turns off the port LEDs.

```
switchxxxxxx# disable ports leds
```

6.27 show ports leds configuration

Use the show port leds configuration EXEC mode command to display whether the LEDs of the ports are enabled or disabled.

Syntax
show ports leds configuration

Command Mode
EXEC mode

Examples
Example 1: The following example displays the status of the port’s LEDs when they are turned on.

```
switchxxxxxx# show ports leds configuration
Port leds are not disabled
```

Example 2: The following example displays the status of the port LEDs when they are turned off.

```
switchxxxxxx# show port leds configuration
Port leds are disabled
```
**SSH Client Commands**

### 7.1 ip ssh-client authentication

Use the **ip ssh-client authentication** command in Global Configuration mode to define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers.

To return to default, use the **no** format of the command.

**Syntax**

```
ip ssh-client authentication {password | public-key {rsa | dsa}}
no ip ssh-client authentication
```

**Parameters**

- **password** — Username and password are used for authentication.
- **public-key rsa** — Username and RSA public key are used for authentication.
- **public-key dsa** — Username and DSA public key are used for authentication.

**Default Configuration**

Username and password are used for authentication by the local SSH clients.

**Command Mode**

Global Configuration

**User Guidelines**

A user can use the **ip ssh-client key** command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.
Example
The following example specifies that, username and public key are used for authentication:

```plaintext
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

### 7.2 ip ssh-client change server password

Use the `ip ssh-client change server password` command in Global Configuration mode to change a password of an SSH client on a remote SSH server.

**Syntax**

```
ip ssh-client change server password server {host | ip-address | ipv6-address} username username old-password old-password new-password new-password
```

**Parameters**

- **host**—DNS name of a remote SSH server.
- **ip-address**—Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **username** — Username of the local SSH clients (1 - 70 characters).
- **old-password** — Old password of the local SSH client (1 - 70 characters).
- **new-password**— New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ".".

**Default Configuration**

N/A

**Command Mode**

Global configuration

**User Guidelines**

Use the command to change a password on a remote SSH server. Use `ip ssh-client password` to change the SSH client password of the switch's SSH client so that it matches the new password set on the remote SSH server.
Example
The following example changes a password of the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client change server password server 10.7.50.155
username john old-password &&&@@@aaff new-password &&&@@@aaee
```

7.3 ip ssh-client key

Use the `ip ssh-client key` command in Global Configuration mode to create a key pair for SSH client authentication by public key (either by generating a key or by importing a key). To enter the private key as encrypted, use the `encrypted ip ssh-client key` command.

To remove a key, use the `no` form of the command.

Syntax

```
ip ssh-client key {dsa | rsa} {generate | key-pair privkey pubkey}
encrypted ip ssh-client key {dsa | rsa} key-pair encrypted-privkey pubkey
no ip ssh-client key [dsa | rsa]
```

Parameters

- `dsa`—DSA key type.
- `rsa`—RSA key type.
- `key-pair`—Key that is imported to the device.
- `privkey`—Plaintext private key.
- `encrypted-privkey`—private key is in encrypted format.
- `pubkey`—The plaintext public key.

Default Configuration
The application creates a key automatically; this is the default key.

Command Mode
Global configuration
**User Guidelines**

When using the keyword `generate`, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword `key-pair`, the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the `no ip ssh-client key` command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

*Table 2* describes the expected behavior of keys, default and users within the various operations.

<table>
<thead>
<tr>
<th>From/To</th>
<th>Show</th>
<th>Show (detailed)</th>
<th>Copy/Upload of Running Config</th>
<th>Copy/Upload of Startup Config</th>
<th>Download text-based CLI (TFTP/Backup)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config</td>
<td>Only user-defined.</td>
<td>N/A</td>
<td>All keys (default and user)</td>
<td>N/A</td>
<td>All keys (default and user)</td>
</tr>
<tr>
<td>Running Config</td>
<td>Keys are not displayed.</td>
<td>All keys (default and user)</td>
<td>N/A</td>
<td>Only user defined.</td>
<td>Same as user configuration</td>
</tr>
<tr>
<td>Text-based CLI (TFTP/Backup)</td>
<td>As it was copied.</td>
<td>N/A</td>
<td>All keys (default and user)</td>
<td>Only user defined.</td>
<td>As a text file.</td>
</tr>
</tbody>
</table>

If no keys are included in text-based configuration file, the device generates its own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

**Examples**

**Example 1** - In the following example, a key pair of the RSA type is created:

```
switchxxxxxx(config)# ip ssh-client key rsa generate
```

The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.

**Example 2** - In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
switchxxxxxx(config)#ip ssh-client key rsa key-pair
```

Please paste the input now, add a period (.) on a separate line after the input

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CUZK18rYrK5+TVxwS4zvbBMc4I31m9cR/1iRTTVlMRuJ++TEr9ssqWy1lTl9d0jzgG0N3jHzp2je5/DUTHZXvYaUzcbBdntsPTJo8dyiBl4YbqYHQgCjUhktxQvloy+luxRJTAAaLVCBAmIU/kMLoEox8/zwjb/ji9WIBiwKBgC2xZ5mQmv0+yo2GUFlwQ5f0ywemMl1J8McTmqDgfVTRrdbxwbs3exVqsfaUY9wa8Le6JXP+DPp4XovEfC/ig1zBSC8SeDm12U7D6HrkAyD9Hhf/r32jukB+5Z7lHPz2Xczs2cl00OwnrToy+YTzjLixyWS7V/IxbB1ipLAEAj1vSCrfMdmMl2xaEfJVzqP01cF8guovsWLteBf/gqHuvbHuNy0tOWEpObKZs1/mTCWppkgcqgrBOOJaYbUFOQJBAMo/cCrkyhiSiV/+2sryeD26NhPEKiak16V
```

```
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGxYtisrn5Ml/BLjO+EGaILgjfWb1xH/WJFMVWXiG4n75MSun2yypbiJvOL13SP0YbQ3eMfOnaN7n8NRMde9hpTNYeEE0ew9Mnjx3KIGxgGpgdCAKNSGS1eq+WJL7WFE1MBotVcIECa4hT+QwugSjHz/PCMH+GwX3AgEj
-----END RSA PUBLIC KEY-----
```

**Example 3** - In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
```
(Need to encrypted SSH client RSA key pair, for example:)

----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxeOjs6OzGRtL4qstmQg1B/4geQb1fa56RdjgHAMEjvUT02elYmNi+m4aTu6mlXPHmY
1X1Xny7jzKhRvgg8EzcppEB003yQzq3khN1756cMg40qbkms7TU0tdqYFEz/h8rJ0QvUFfh
BsE03e16E/OProWgK43WTzed5uyPeOoMXR9BCuxPUJc2UeqQVM21Jt5OM0fbVt0S6oqXhG
sEEdOT1h1DwHw97FecV7x+hEnPfzFGrmbrUxcoxOxlkFsuCNo3/94PHK8zEXyNtrr2KoCDQ
qFRuM8uecpjmDh6M02GURUVstctohEWEIVCIOr5SBcicaxv5o8jIzXMrJA==
-----END RSA PRIVATE KEY-----

----BEGIN RSA PUBLIC KEY-----
MIGHA0GBALLOeh3css8tBL8ujFt3trcX0XJyJL1xxt4sGp8Q3ExISRN25+Mcac6tobgIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5y04xG6Fp42nhHicgie+YTSlo309E2kiXa
QeJtldnYL/r3uTIRGGbX5nxwtfWwpEgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----

**Example 4** - In the following example, a DSA key pair is removed:

```plaintext
switchxxxxxx(config)# no ip ssh-client key dsa
```

**Example 5** - In the following example, all key pairs (RSA and DSA types) are removed.

```plaintext
switchxxxxxx(config)# no ip ssh-client key
```

### 7.4 ip ssh-client password

Use the **ip ssh-client password** command in Global Configuration mode to configure the password for SSH client authentication by password. To enter the password as encrypted, use the **encrypted ip ssh-client password** command. To return to default, use the **no** form of the command.

**Syntax**

- `ip ssh-client password string`
- `encrypted ip ssh-client password encrypted-string`
no ip ssh-client password

Parameters

- **string**— Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ".".
- **encrypted-string**— Password for the SSH client in encrypted form.

Default Configuration

The default password is anonymous.

Command Mode

Global configuration

User Guidelines

If authentication is configured to use a password (using the command `ip ssh-client authentication`), use the `ip ssh-client password` command to define the password. If the encrypted key-word is used, the password must be in the encrypted form.

Use the command `ip ssh-client change server password` to change the password on the remote SSH server so that it will match the new password of the SSH client.

Example

The following example specifies a plaintext password for the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client password &&&&111aaff
```

### 7.5  ip ssh-client server authentication

Use the `ip ssh-client server authentication` command in Global Configuration mode to enable remote SSH server authentication by the SSH client.

To disable remote SSH server authentication, use the `no` form of the command.

Syntax

- `ip ssh-client server authentication`
- `no ip ssh-client server authentication`
Parameters
None

Default Configuration
SSH server authentication is disabled

Command Mode
Global configuration

User Guidelines
When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the `ip ssh-client server fingerprint` command to configure trusted SSH servers.

Example
The following example enables SSH server authentication:

```
switchxxxxxx(config)# ip ssh-client server authentication
```

### 7.6  `ip ssh-client server fingerprint`

Use the `ip ssh-client server fingerprint` command in Global configuration mode to add a trusted server to the Trusted Remote SSH Server Table. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the `no` form of the command.

**Syntax**

```
ip ssh-client server fingerprint [host | ip-address] fingerprint
no ip ssh-client server fingerprint [host | ip-address]
```

**Parameters**

- host—DNS name of a SSH server.
SSH Client Commands

- **ip-address**—Specifies the address of a SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

- **fingerprint**—Fingerprint of the SSH server public key (32 Hex characters).

**Default Configuration**

The Trusted Remote SSH Server table is empty.

**Command Mode**

Global configuration

**User Guidelines**

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server’s public key, it calculates the received key’s fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The `no ip ssh-client server fingerprint` command removes all entries from the Trusted Remote SSH Server table.

**Example**

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC78978DC88A988127897BCBB789788
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
```

### 7.7 ip ssh-client source-interface

Use the `ip ssh-client source-interface` Global Configuration mode command to specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers. Use the `no` form of this command to restore the default configuration.
SSH Client Commands

7.8 ipv6 ssh-client source-interface

Use the `ipv6 ssh-client source-interface` Global Configuration mode command to specify the source interface which IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers. Use the `no` form of this command to restore the default configuration.

Syntax

`ipv6 ssh-client source-interface interface-id`

Parameters

`interface-id`—Specifies the source interface.
no ipv6 ssh-client source-interface

Parameters

interface-id—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

switchxxxxxx(config)# ipv6 ssh-client source-interface vlan 100

7.9  ip ssh-client username

Use the ip ssh-client username command in Global Configuration mode to configure the SSH client username of the switch.

To return to default, use the no form of the command.

Syntax

ip ssh-client username string
no ip ssh-client username
SSH Client Commands

Parameters

string— Username of the SSH client. The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global configuration

User Guidelines

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

```
switchxxxxxx(config)# ip ssh-client username jeff
```

7.10 show ip ssh-client

Use the show ip ssh-client command in Privilege EXEC mode to display the SSH client credentials, both default and user-defined keys.

Syntax

show ip ssh-client
show ip ssh-client {mypubkey | key} {dsa | rsa}

Parameters

- dsa— Specifies displaying the DSA key type.
- rsa— Specifies displaying the RSA key type.
- mypubkey— Specifies that only the public key is selected to be displayed.

Command Mode

Privileged EXEC mode
User Guidelines

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

Example

Example 1. The following example displays the authentication method and the RSA public key:

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKgBN1WmXnYkUf5o2jGY3QoMGDvNipQvdN3YmwLUBiKk3lWvVwFB3N2KSa7fUBjolkaldjnsQKTKZiu4V+IL5rds/bD6LOEkJbjUzOjmp9h1Ikh9uc0ce232xMtRhn0RLrXL
aRyxYszO5FuiTo6xW8=
---- END SSH2 PUBLIC KEY ----
```

Example 2. The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
```
Key Source: User Defined

---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehv5x0w0J0rzZdsoSOXxbETW67o8V8dUJ/z+zho9Fiko5xy8znD1a0DHtb1Q+Yp7Stxy1thHNXF1YLFkD1G4T6JYrdHey140mele9e4NnCRleaog2PF3UGFZia6bxrGTQf3gQq287Yisk/gF+1VAAAAFQDB8D5c
vhWHTZDPFx0D2s9Rd7NBvQAAAAAEALN92+Bb7D4KLYk3IwRbXblXdkPggA4pfW9vGFJO/RHd+NJb4eo1D+0dix6tXwYGN7PKS5R/FXPNxwHPacj9uL1Jn2AWQ2dsknfi+i/FAAvioUPkmdMc0zuWoSOEsSNhVDtx3WdVcGcBq9cetzMr0KWOoc3jmJ80qadxTRHtUAAACB
AN7CY+KKvlHpRzFwQm7HK9bb1LAc02KwaoXnadFgeptNBQeSXGlvo+JsphVMBJc9HS
n24VYtYsMu74qXviYziVucWKjKeb11juqfn0G0D1B3VmxhLmxnAz643Wk4277dLM5sY29oue4x22PmCh5VGP+CDqzCM41oWgV

---- END SSH2 PUBLIC KEY ----

---- BEGIN SSH2 PRIVATE KEY ----
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehv5x0w0J0rzZdsoSOXxbETW67o8V8dUJ/z+zho9Fiko5xy8znD1a0DHtb1Q+Yp7Stxy1thHNXF1YLFkD1G4T6JYrdHey140mele9e4NnCRleaog2PF3UGFZia6bxrGTQf3gQq287Yisk/gF+1VAAAAFQDB8D5c
vhWHTZDPFx0D2s9Rd7NBvQAAAAAEALN92+Bb7D4KLYk3IwRbXblXdkPggA4pfW9vGFJO/RHd+NJb4eo1D+0dix6tXwYGN7PKS5R/FXPNxwHPacj9uL1Jn2AWQ2dsknfi+i/FAAvioUPkmdMc0zuWoSOEsSNhVDtx3WdVcGcBq9cetzMr0KWOoc3jmJ80qadxTRHtUAAACB
AN7CY+KKvlHpRzFwQm7HK9bb1LAc02KwaoXnadFgeptNBQeSXGlvo+JsphVMBJc9HS
n24VYtYsMu74qXviYziVucWKjKeb11juqfn0G0D1B3VmxhLmxnAz643Wk4277dLM5sY29oue4x22PmCh5VGP+CDqzCM41oWgV

---- END SSH2 PRIVATE KEY ----

Example 3. The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
```
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method: DSA key
Username: anonymous (default)
Password: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf92BAU5nsxSwiw=

7.11 show ip ssh-client server

Use the `show ip ssh-client server` command in Privilege EXEC Configuration mode to display the SSH remote server authentication method and the Trusted Remote SSH Server table.

Syntax

`show ip ssh-client server [host | ip-address]`

Parameters

- `host` — DNS name of an SSH server.
- `ip-address` — IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

N/A

Command Mode

Privilege EXEC configuration mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Example

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:
switchxxxxx# **show ip ssh-client server**

SSH Server Authentication is enabled

**server address: 11.1.0.1**

**server address: 192.165.204.111**

**server address: 4002:0011::12**

**Example 2** - The following example displays the authentication method and DSA private key in encrypted format:

switchxxxxx# **show ip ssh-client key DSA**

**Authentication method:** DSA key

**Username:** john

**Key Source:** Default


---- BEGIN SSH2 PUBLIC KEY ----

Comment: RSA Public Key

AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8d1UJ/z+zHo9Fiko5Xybo2nDIaBDHtb1Q+Yp7Stxy1HnXFlYlfKDI1G76JYrdH
YI140mledg9e4NnCRleaqrtiP3UGFzia6XrGTQf3gJq2e7Yisk/gF+1VAAAADFQdb8D5c
vwHTZDPfx0D2s9Rd7NBvQAAAIEAI9N2+BB7D4KLYK131wRbXblwXdkPggAApfjtw9vGf
J0/Rd+NjB4eo1D+0dix6txYGN7P978/SF7PXwHPapcj9u1Jn2AWQ2dsknf+i/FAA
vioUPkm đóSw0S0EsSnhVDxt3WdvVcBcBq9ctzrtOKW0ocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHrpFwdQm7HK9bb1La2KwaoXnadFgeptNBQesXG1vO+JsvphVMBjC9HS
n24YYtYtsMu74qXviYjiVucWKjKjKEb11juqnf0Gd1B3VmvxHLmxnAz643W4227dLM5
sY29ouezv4Xz2PuMch5VGFPCQdzCM4loWgV

---- END SSH2 PUBLIC KEY ----

---- BEGIN SSH2 PRIVATE KEY ----

Comment: DSA Private Key

AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client

Authentication method: password (default)
Username: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```

--- END SSH2 PRIVATE KEY ----
8.1 stack master

Use the stack master Global mode command to configure a specific unit to be the stack master (forced master).

Use the no form of this command to restore the default configuration.

Syntax

stack master unit unit-id

no stack master

Parameters

unit-id—Specifies the new master unit number. (Range: 1, 2)

Default Configuration

The default is no forced master, and the master is selected during the master election process.

Command Mode

Global Configuration mode

Example

The following example forces the stack master to be unit 2.

switchxxxxxx(config)# stack master unit 2
8.2  stack standalone

Use the `stack standalone` Privileged EXEC command to change all units in a stack to Standalone mode, meaning that they are no longer part of a stack. The new configuration takes place after reset.

Syntax

```
stack standalone [reboot]
```

Parameters

reboot—Perform reboot on all connected units in the stack, after changing the mode to Standalone.

Default Configuration

Reboot is not performed.

Command Mode

Privileged EXEC mode

User Guidelines

The Startup Configuration file is deleted during the first bootup of the device in Standalone mode. When setting the device to Standalone mode, a warning about this deletion is displayed to the user.

Example

The following example sets the stack mode to Standalone in all units in a stack and then performs reboot.

```
switchxxxxxx# stack standalone reboot
```

Changing the switch from stacking to standalone will *delete* the startup configuration file and reset the device right after that. It is highly recommended that you will backup it before changing to standalone, continue ? (Y/N) [N]

8.3  stack native

Use the `stack native` Privileged EXEC command to perform one of the following actions:
- Change a single standalone unit to Native Stacking mode (see User Guidelines for an explanation of this mode).

- Configure stack parameters, such as the type of stacking ports and their speeds for the units in a stack.

- Set the unit number after reboot. If there is more than one unit in the stack, only \texttt{unit-id-auto} can be selected.

The new configuration takes place after reboot.

This command configures the entire stack (if a stack exists) as opposed to the \texttt{native} command, which configures a single unit.

\textbf{Syntax}

\texttt{Sx500 devices: stack native \{s1-s2|s3-s4\} \{1g / 5g / auto\} [1 - 8 | unit-id-auto] [reboot]}

\texttt{SG500X/ESW2-550X devices): stack native \{s1-s2-5g / s1-s2-xg\} \{1g / 5g / xg / auto\} [1 - 8 | unit-id-auto] [reboot]}

\texttt{SG500XG devices): stack native \{xg-1—xg-16\} \{xg-1—xg-16\} \{1g / xg / auto\} [1—8 | unit-id-auto] [reboot]}

\textbf{Parameters}

\textbf{For Sx500 devices:}

- **Stack Port Type:**
  - \texttt{s1-s2}—Set the stack ports to be \textit{S1-S2 Combo-1G}.
  - \texttt{s3-s4}—Set the stack ports to be \textit{S3-S4 5G Stack}.

- **Speed:**
  - \texttt{1g}—Force stack port speed to be 1G.
  - \texttt{5g}—Force stack port speed to be 5G. Relevant if \textit{S3-S4 5G Stack is selected}
  - \texttt{auto}—Configure the stack port with the maximum speed possible on the cable and port automatically. This option is relevant only if \textit{S3-S4 5G Stack is selected}

\textbf{For SG500X/ESW2-550X devices:}

- **Stack Port Type:**
  - \texttt{s1-s2-5g}—Set the stack ports to be \textit{S1-S2 5G Stack}.
- **s1-s2-xg**—Set the stack ports to be *S1-S2 XG Stack*.

  - **Speed:**
    - **1g**—Force stack port speed to be 1G.
    - **5g**—Force stack port speed to be 5G. Relevant if *S1-S2 5G Stack is selected*.
    - **xg**—Force stack port speed to be 10G. Relevant if S1-S2 XG Stack is selected.
    - **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically.

For **SG500XG devices:**

- **Stack Port Type:**
  - **XG-1-XG-16**—Set the stack port to be *XG-1/XG-2/.../XG-16*. *Two stack ports needs to be selected.*

- **Speed:**
  - **1g**—Force stack port speed to be 1G.
  - **xg**—Force stack port speed to be 10G.
  - **auto**—Configure the stack port with the maximum speed supported by the Gigabit Interface Converter (GBIC) inserted.

- **Unit Numbering:**
  - To assign unit numbers to the units in the stack, set:
    - **unit-id-auto**—Perform automatic numbering of units in stack.
    - **1 - 8**—Unit number that can be used only if the current stack mode is standalone or if there is only one unit in the stack. This parameter specifies the unit ID of this unit when it becomes part of a stack.

  **Note:** If the user does not enter a unit ID or **unit-id-auto**, the unit ID of all units are retained.

  **Reboot Unit:**
  - **Reboot**—Perform reboot on all units, after setting the new stack values on all units.
Default Configuration
N/A

Command Mode
Privileged EXEC mode

User Guidelines
For proper stack connection, the stack ports and the stack ports speed should be the same on all the stack units.

Examples

Example 1 (For Sx500 devices)—The following example sets the stack parameters in all units of a stack consisting of Sx500 units. Stacking ports are set to S1-S2 Combo-1G and 5G speed. Renumbering is set to automatic renumbering of the stack. Reboot is performed automatically after the command.

```
switchxxxxxx# stack native s1-s2 5G unit-id-auto reboot
```

Example 2 (For Sx500 devices)—The following example sets the stack parameters in all units of a stack consisting of Sx500 units. Stacking ports are set to S3-S4 5G Stack and to the maximum speed possible. Renumbering is set to automatic renumbering of the stack. Reboot is performed automatically after the command.

```
switchxxxxxx# stack native s3-s4 auto unit-id-auto reboot
```

Example 3 (For SG500X/ESW2-550X devices)—The following example sets the stack parameters in all units of a stack consisting of SG500X/ESW2-550X units. Stacking ports are set to S1-S2 5G Stack and to 1G speed. Renumbering is set to automatic renumbering of the stack. Reboot is performed automatically after the command.

```
switchxxxxxx# stack native s1-s2-5g 1g unit-id-auto reboot
```

Example 4 (For SG500X/ESW2-550X devices)—The following example sets a standalone unit to be a stack member with the unit number 3, with no automatic
reboot. Stacking ports are set to be of type *S3-S4 XG Stack* with speed automatically set to the highest speed supported.

```
switchxxxxxx# stack native s1-s2-xg auto 3
```

**Example 5 (For SG500XG devices)**—The following example sets a standalone unit to be a stack member with the unit number 3, with no automatic reboot. Stacking ports are set to be *XG-1 and XG-2* with speed automatically set to the highest speed supported.

```
switchxxxxxx# stack native xg-1 xg-2 auto 3
```

### 8.4 stack basic-hybrid

Use the `stack basic-hybrid` Privileged EXEC command to perform one of the following actions:

- Change a single standalone unit or stack units to Basic Hybrid mode (see User Guidelines for an explanation of this mode).
- Configure stack parameters, such as speeds for the units in a stack. If there is more than one unit in the stack, only `unit-id-auto` can be selected.

The new configuration takes place after reboot.

**Syntax**

```
stack basic-hybrid {1g | 5g | auto} [1 - 8 | unit-id-auto] [reboot]
```

*(Sx500)* This command configures the stack port type as: *S3-S4 5G Stack*.

*(SG500X/ESW2-550X)* This command configures the stack port type as: *S1-S2 5G Stack*.
Parameters

Speed:

- **1g**—Force stack port speed to be 1G.
- **5g**—Force stack port speed to be 5G.
- **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically.

Unit Numbering:

- To assign unit numbers to the units in the stack, set:
  - `unit-id-auto`—Perform automatic numbering of units in stack.
  - `1 - 8` —Unit number that can be used only if the current stack mode is Standalone or if there is only one unit in the stack. This parameter specifies the unit ID of this unit when it becomes part of a stack.

  **Note:** If the user does not enter a unit ID or `unit-id-auto`, the unit ID of all units are retained.

Reboot Unit:

- **Reboot**—Perform reboot on all units, after setting the new stack values on all units.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

If the stack is in Basic Hybrid mode both Sx500 and SG500X/ESW2-550X units can only be used without VRRP and RIP.

Examples

The following example sets the stack parameters in all units of a stack consisting of Sx500 units. Stacking ports are set to **S3-S4 5G** and 5G speed. Renumbering is set to automatic renumbering of the stack. Reboot is performed automatically after the command.
Use the `stack advanced-hybrid` Privileged EXEC command to perform one of the following actions:

- Change a single standalone unit to Advanced Hybrid mode (see User Guidelines for an explanation of this mode).
- Configure stack parameters, such as speeds for all the units in a stack.

The new configuration takes place after reboot.

**Syntax**

```
stack advanced-hybrid {1g | 5g | auto} [1 - 8] [reboot]
```

Note that executing this command configures the stack port type as following:

- For Sx500 unit: *S3-S4 5G Stack is selected*
- For SG500X/ESW2-550X unit: *S1-S2 5G Stack is selected*

**Parameters**

- **Speed:**
  - 1g—Force stack port speed to be 1G.
  - 5g—Force stack port speed to be 5G.
  - auto—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering:** Unit number that can be used only if the current stack mode is standalone or if there is only one unit in the stack. This parameter specifies the unit ID of this unit when it becomes part of a stack.

- For Sx500 unit: 3 - 8.
For SG500X/ESW2-550X unit: 1 - 8.

**Note**: If the user does not enter a unit ID, the unit ID of all units are retained. If the unit ID prior to issuing this command is auto, the user must specify a unit ID.

**Reboot Unit:**

- **Reboot**—Perform reboot on all units, after setting the new stack values on all units.

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

In Advanced Hybrid mode both Sx500 and SG500X/SG500XG/ESW2-550X units can be used in a stack with VRRP and RIP. Note that the Sx500 units can be a slave only in this mode.

This command sets the stacking mode and speed parameter. It can be executed on a standalone unit, or in any stacking mode and changes all units stacking mode to Advanced Hybrid and sets the speed of all of them to Auto. **NOTE**: if the current stack master or backup unit is Sx500, the user receives an error message since these units cannot be configured as 1 / 2 in Advanced Hybrid mode.

**Example**

The following example sets the stack port speed to be auto in all the stack units. Reboot is performed automatically after the command.

```
switchxxxxxx# stack advanced-hybrid auto reboot
```

---

8.6 **stack advanced-hybrid-xg**

- **Note**: This command is not found on Sx500 devices.
Use the `stack advanced-hybrid-xg` Privileged EXEC command to perform one of the following actions:

- Change a single standalone unit to Advanced Hybrid XG mode (see User Guidelines for an explanation of this mode).
- Configure stack parameters, such as speeds for the units in a stack.

The new configuration takes place after reboot.

**Syntax**

SG500X/ESW2-550X devices): `stack advanced-hybrid-xg {1g | xg | auto} [1 - 8 | unit-id-auto] [reboot]`

SG500XG devices): `stack advanced-hybrid-xg {xg-1—xg-16} {xg-1—xg-16} {1g | xg | auto} [1—8 | unit-id-auto] [reboot]`

**Parameters**

**Speed:**

- 1g—Force stack port speed to be 1G.
- xg—Force stack port speed to be 10G.
- auto—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering:** To assign unit numbers to the units in the stack, set:

- `unit-id-auto`—Perform automatic numbering of units in stack.
- 1 - 8 —Unit number that can be used only if the current stack mode is standalone or if there is only one unit in the stack. This parameter specifies the unit ID of this unit when it becomes part of a stack.

**Note:** If the user does not enter a unit ID or `unit-id-auto`, the unit ID of all units are retained.

**Reboot Unit:**

- Reboot—Perform reboot on all units, after setting the new stack values on all units.

**Default Configuration**

N/A
Command Mode
Privileged EXEC mode

User Guidelines
This mode is used when connecting SG500X/ESW2-550X and SG500XG units in stack. The MAC Address Table size in this case will be lowered to 16K. Both unit types can become the stack Master.

In the SG500X/ESW2-550X unit, the stack ports will be s1-s2-xg.

Example
The following example sets the stack ports of an SG500XG device to be xg-1 and xg-2 and stack ports speed to be auto in a stack unit. Reboot is performed automatically after the command.

```
switchxxxxxx# stack advanced-hybrid-xg xg-1 xg-2 auto reboot
```

8.7 stack reset

Use the `stack reset` Privileged EXEC command to reset either a standalone switch, a specific unit in a stack, or all units in a stack to default factory stack parameter values (see the User Guidelines). Note that the command also resets unit IDs to their factory defaults.

The new configuration takes place after reboot. If the stack mode is changed after this operation (relevant whenever the stack mode prior to running this command is not native mode), the startup configuration file is deleted.

Syntax
```
stack reset [unit-id]
```

Parameters
unit-id—Unit to configure. (Range: 1–8)

Default Configuration
Operates on entire stack if `unit-id` is not specified.

Command Mode
Privileged EXEC mode
User Guidelines

The following describes the default configuration.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Stacking Mode</th>
<th>Stack Unit Mode</th>
<th>Stack Ports</th>
<th>Stack Ports Speed</th>
<th>System Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG500X G</td>
<td>Stacking</td>
<td>N/R</td>
<td>N/R</td>
<td>N/R</td>
<td>L2/L3-enabled mode</td>
</tr>
<tr>
<td>SG500X/ESW2-550X</td>
<td>Native</td>
<td>S1-S2 10G Stack</td>
<td>s1: Auto, s2: Auto</td>
<td></td>
<td>L3-enabled mode</td>
</tr>
<tr>
<td>Sx500</td>
<td>Stacking</td>
<td>Native</td>
<td>S3-S4 5G Stack (directly-attached)</td>
<td>s3: Auto, s4: Auto</td>
<td>L2 Mode</td>
</tr>
</tbody>
</table>

Example:

**Example 1**—The following examples return the factory stack default values for unit 3.

```
switchxxxxxx# stack reset 3
```

**Example 2**—The following examples return the factory stack default values for all units in the stack.

```
switchxxxxxx# stack reset
```

Note that since the system stack mode will revert to default (Native Stack mode), the startup configuration file will be deleted when the system is rebooted.

8.8 stack unit

The `stack unit` Privileged EXEC command places the user in the context of the specified stack unit.

Syntax

```
stack unit [unit-id]
```

Parameters

**unit-id**—Select a specific unit. All commands after this command refer to this unit. In Standalone mode or if there is only a single unit in the stack, this parameter cannot be entered. (Range: 1–8).

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

**Example 1 (For Sx500 devices)—Enter Stack Unit mode on unit 2 and configure it.**

```
switchxxxxx# stack unit 2
switchxxxxx(sx500)# native s1-s2 5g unit-id-auto reboot
```

**Example 2 (For Sx500 devices)—Enter Stack Unit mode on a device with only one unit in it.**

```
switchxxxxx# stack unit
switchxxxxx(sx500)# native s1-s2 5g unit-id-auto reboot
```

**Example 3 (For SG500X/ESW2-550X devices)—Enter Stack Unit mode on unit 2 and configure it.**

```
switchxxxxx# stack unit 2
switchxxxxx(sg500x)# native s1-s2-5g 5g unit-id-auto reboot
```

**Example 4 (For SG500X/ESW2-550X devices)—Enter Stack Unit mode on a device with only one unit in it.**

```
switchxxxxx# stack unit
switchxxxxx(sg500x)# native s1-s2-5g 5g unit-id-auto reboot
```

**Example 5 (For SG500XG devices)—Enter Stack Unit mode on a device with only one unit in it.**

```
switchxxxxx# stack unit
```
8.9 native

Use the **native** Privileged EXEC command to perform one of the following actions for a single unit:

- Change a single standalone unit to Native stack mode (see User Guidelines for an explanation of Native stack mode).
- Configure stack parameters such as, the type of stacking ports and their speeds.

The new configuration takes place after reboot.

This command configures only a single unit as opposed to **stack native**, which configures the entire stack.

**Syntax**

Sx500 devices: native {s1-s2 | s3-s4} {1g | 5g | auto} [1-8 | unit-id-auto] [reboot]

SG500X/ESW2-550X devices: native {s1-s2-5g | s1-s2-xg} {1g | 5g | xg | auto} [1—8 | unit-id-auto] [reboot]

SG500XG devices: native {xg-1—xg-16} {xg-1—xg-16} {1g | xg | auto} [1—8 | unit-id-auto] [reboot]

**Parameters**

Sx500 devices:

- Stack Port Type:
  - s1-s2—Set the stack ports to be *S1-S2 Combo-1G*.
  - s3-s4—Set the stack ports to be *S3-S4 5G Stack*.

- Speed:
  - 1g—Force stack port speed to be 1G.
  - 5g—Force stack port speed to be 5G. Relevant if *S3-S4 5G Stack is selected*
- **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically. This option is relevant only if *S3-S4 5G Stack* is selected.

**SG500X/ESW2-550X devices:**

- **Stack Port Type:**
  - s1-s2-5g—Set the stack ports to be *S1-S2 5G Stack*.
  - s1-s2-xg—Set the stack ports to be *S1-S2 XG Stack*.

- **Speed:**
  - 1g—Force stack port speed to be 1G.
  - 5g—Force stack port speed to be 5G. Relevant if *S1-S2 5G Stack is selected*.
  - xg—Force stack port speed to be 10G. Relevant if S1-S2 XG Stack is selected.
  - auto—Configure the stack port with the maximum speed possible on the cable and port automatically.

**For SG500XG devices:**

- **Stack Port Type:**
  - xg-1-xg-16—Set the stack port to be xg-1 | xg-2 | ... | xg-16. Two stack ports needs to be selected.

- **Speed:**
  - 1g—Force stack port speed to be 1G.
  - xg—Force stack port speed to be 10G. Relevant if S1-S2 XG Stack is selected.
  - auto—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering:**

- To assign unit numbers to the unit, set:
  - unit-id-auto—Perform automatic numbering of the unit. The result after reboot could be that the unit ID is retained or that the unit is assigned another ID depending on the IDs of the other units in the stack. For
example, if the current unit ID is 4 and the other units are 1 and 2. After reboot, this unit is assigned 3.

- **1-8**—Specifies the unit ID of this unit after reboot.

**Note:** If the user does not enter a unit ID or **unit-id-auto**, the unit ID is retained.

**Reboot Unit:**

- **Reboot**—Perform reboot on unit after setting new values.

**Default Configuration**

N/A

**Command Mode**

Stack Unit mode

**User Guidelines**

The following describes system functionality when units are switched from Standalone to Native mode:

- **From Standalone to Native**—Startup configuration file is retained only if unit ID was set to 1 by the user.

  In order not to lose the configuration, the startup config file must be saved to backup config or uploaded to an TFTP server. It should not be restored without careful verification, since there might be irrelevant interfaces in the configuration.

- **From Native to Standalone**—Regardless of what system mode the device is in, the new system mode after reset will be L2, unless the system mode is set manually to L3 after stack mode configuration, but before the reboot.

For proper stack connection, the stack ports and the stack ports speed should be the same on all the stack units.

**Examples**

**Example 1 (For Sx500 devices)**—The following example sets the stack parameters in a unit. Stacking ports are set to *S1-S2 5G Stack* and to 5G speed. Renumbering is set to automatic renumbering of the stack. Reboot is performed.
Example 2 (For SG500X/ESW2-550X devices)—The following example sets the stack parameters in unit 1. Stacking ports are set to S1-S2 5G Stack and to 5G speed. Renumbering is set to automatic renumbering of the stack. Reboot is performed.

```
switchxxxxxx# stack unit 1
switchxxxxxx(sg500x)# native s1-s2-5g 5g unit-id-auto reboot
```

For proper stack connection, ensure that the stack ports and the stack ports speed are the same on all the stack units. Do you want to continue and reboot the stack unit? (Yes, No)

Example 3 (For SG500X/ESW2-550X devices)—The following example sets the stack parameters in unit 1. Stacking ports are set to be of type 5G with auto setting speed. The unit is renumbered to 3. Reboot is performed automatically after the command.

```
switchxxxxxx# stack unit 1
switchxxxxxx# native s1-s2-5g auto 3 reboot
```

Example 4 (For SG500XG devices)—The following example sets the stack parameters in unit 1. Stacking ports are set to be xg-1 and xg-16 with auto setting speed. The unit is renumbered to 3. Reboot is performed automatically after the command.

```
switchxxxxxx# stack unit 1
switchxxxxxx# native xg-1 xg-16 auto 3 reboot
```

8.10 standalone

The standalone Stack Unit mode command changes the stack parameters for a standalone switch. The new configuration takes place after reset.

**Syntax**

Sx500: standalone [switch | router] [reboot]
SG500X/ESW2-550X and SG500XG: standalone [reboot]

Parameters

- `switch | router`—Sets the L2/L3 system mode when setting the unit to Standalone mode. If the user does not enter a value, the current mode is retained.
- `reboot`—Reboot the unit.

Default Configuration

If neither switch nor router is specified, the current mode of the device is retained.

Command Mode

Stack Unit mode

User Guidelines

The startup configuration is removed when switch the stack unit mode to Standalone mode. The L2/L3 system mode of the switch can be modified by the `set system` command.

Examples

Example 1 (for Sx500 devices)—The following example sets unit 2 to be a standalone unit for an Sx500 unit (this type of device can be in either router mode or switch mode):

```
switchxxxxxx# stack unit 2
switchxxxxxx(sx500)# standalone switch reboot
```

Example 2 (for SG500X/ESW2-550X or SG500XG devices)—The following example sets unit 2 to be a standalone unit:

```
switchxxxxxx# stack unit 2
switchxxxxxx(sg500x)# standalone reboot
```
Use the `basic-hybrid` Stack Unit mode command to perform one of the following actions for a single unit:

- Change a single unit to Basic Hybrid stack mode (see User Guidelines for an explanation of Native stack mode).
- Configure stack parameters such as the speed of the stacking ports.

The new configuration takes place after reboot.

This command configures only a single unit. To configure the entire stack use `stack basic-hybrid`, which configures the entire stack.

**Syntax**

```
basic-hybrid {1g | 5g | auto} [1-8 | unit-id-auto] [reboot]
```

**Sx500**: This selects the S3-S4 5G stack port.

**SG500X/ESW2-550X**: This selects the S1-S2 5G stack port.

**Parameters**

**Speed**:

- **1g**—Force stack port speed to be 1G.
- **5g**—Force stack port speed to be 5G.
- **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering**:

- To assign unit numbers to the unit, set:
  - **unit-id-auto**—Perform automatic numbering of the unit. The result after reboot could be that the unit ID is retained or that the unit is assigned another ID depending on the IDs of the other units in the stack. For
example, if the current unit ID is 4 and the other units are 1 and 2. After reboot, this unit is assigned 3.

- **1-8** —Specifies the unit ID of this unit after reboot.

**Note:** If the user does not enter a unit ID or `unit-id-auto`, the unit ID is retained.

**Reboot Unit:**

- **Reboot**—Perform reboot on unit after setting new values.

**Default Configuration**

N/A

**Command Mode**

Stack Unit mode

**User Guidelines**

The following describes system functionality when units are switched to basic-hybrid mode:

- **From Standalone or Native to Basic-Hybrid**—For Sx500 units, startup configuration file is retained only if unit ID was set to 1 by the user. For SG500X/ESW2-550X, startup configuration is removed.

- **From Advanced-Hybrid to Basic-Hybrid**—Startup configuration file is removed in SG500X/ESW2-550X units (The configuration file does not exist in Sx500 in advanced mode since the Sx500 unit can be slave only)

**Example**

The following example sets the speed parameter in unit 1 (SG500X unit) to be 5G. Reboot is performed.

```
switchxxxxxx#stack unit 1
switchxxxxxx(sg500x)#basic-hybrid 5g reboot
```

For proper stack connection, ensure that the stack ports and the stack ports speed are the same on all the stack units. Do you want to continue and reboot the stack unit? (Yes, No)
8.12 advanced-hybrid

Use the Advanced-Hybrid stack unit mode command to perform one of the following actions for a single unit:

- Change a single unit to Advanced Hybrid stack mode.
- Configure stack parameters such as speeds.

The new configuration takes place after reboot.

Syntax

```sh
advanced-hybrid {1g | 5g | auto} [1-8] [reboot]
```

**Sx500**: This selects the S3-S4 5G stack port.

**SG500X/ESW2-550X**: This selects the S1-S2 5G stack port.

**Parameters**

**Speed:**

- **1g**—Force stack port speed to be 1G.
- **5g**—Force stack port speed to be 5G.
- **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering:**

This parameter specifies the unit ID of this unit when it becomes part of a stack.

- **For Sx500 unit**: 3 - 8.
- **For SG500X/ESW2-550X unit**: 1 - 8.

**Note**: If the user does not enter a unit ID, the unit ID is retained. If the unit ID prior to issuing this command is auto, the user must specify a unit ID.
Reboot Unit:

- **Reboot**—Perform reboot on unit after setting new values.

Default Configuration

N/A

Command Mode

Stack Unit mode

User Guidelines

The following describes system functionality when units are switched to basic-hybrid mode:

- **From Standalone or Native to Advanced Hybrid**—Startup configuration file is removed. For Sx500 units, startup configuration file is retained only if unit ID was set to 1 by the user. For SG500X/ESW2-550X, startup configuration is removed.

- **From Basic Hybrid or Advanced Hybrid to Basic Hybrid**—For SG500X units, startup configuration file is retained only if unit ID was set to 1 by the user. For Sx500, startup configuration is removed.

Example

The following example sets the unit 1 (Sx500 unit) to be 5G with unit id 3. Reboot is performed.

```
switchxxxxxx#stack unit 1
switchxxxxxx(sx500)#advanced-hybrid 5g 3 reboot
```

For proper stack connection, ensure that the stack ports and the stack ports speed are the same on all the stack units. Do you want to continue and reboot the stack unit? (Yes, No)
8.13 advanced-hybrid-xg

Use the `advanced-hybrid-xg` stack unit mode command to perform one of the following actions for a single unit:

- Change a single unit to Advanced Hybrid XG stack mode.
- Configure stack parameters, such as speeds for the units in a stack.

The new configuration takes place after reboot.

**Syntax**

SG500X/ESW2-550X devices): advanced-hybrid-xg {1g / xg / auto} [1—8 | unit-id-auto] [reboot]

SG500XG devices): advanced-hybrid-xg {xg-1—xg-16} {xg-1—xg-16} {1g | xg | auto} [1-8 | unit-id-auto] [reboot]

**Parameters**

**Speed:**

- **1g**—Force stack port speed to be 1G.
- **xg**—Force stack port speed to be 10G.
- **auto**—Configure the stack port with the maximum speed possible on the cable and port automatically.

**Unit Numbering:** To assign unit numbers to the units in the stack, set:

- **unit-id-auto**—Specifies the unit ID of this unit when it becomes part of a stack.

  **Note:** If the user does not enter a unit ID, the unit ID is retained.

**Reboot Unit:**

- **Reboot**—Perform reboot on unit after setting new values.

This command is not found on Sx500 devices.
Default Configuration
N/A

Command Mode
Stack Unit mode

User Guidelines
The following describes system functionality when units are switched to Advanced-Hybrid-XG mode:

- **From Standalone, Native, Basic Hybrid or Advanced Hybrid to Advanced Hybrid XG**—Startup configuration file is retained only if unit ID was set to 1 by the user.
- **From Advanced Hybrid XG to other mode**—Startup configuration is removed

Example
The following example sets the SG500X unit 1 to be 10G with unit ID 3. Reboot is performed.

```
switchxxxxxx#stack unit 1
switchxxxxxx#advanced-hybrid xg 3 reboot
```

For proper stack connection, ensure that the stack ports speed are the same on all the stack units. Do you want to continue and reboot the stack unit? (Yes, No)

8.14 show stack

The **show stack** EXEC mode command displays the current stack operational and administrative (set-after reboot) parameters in all units.

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

Parameters
- **unit-id**—Display information for specified unit
- **all**—Display information for all units
### Default Configuration

If no parameter is supplied, all units are displayed (as in all).

### Command Mode

EXEC mode

### Examples

**Example 1**—Display the stack information for an entire stack with one SG500XG device and one SG500X device.

```
SG500X-Native#show stack
Current stack mode is : native
Unit Model Name   MAC Address       Software  Master   Unit No./ Mode After Status
                  Mode After Reboot
---- ------- ----------------- --------- -------- ------------- ------
1    SG500X-48P  00:00:44:55:66:77 1.3.5.34  Enabled Auto,         master
      Native
2    SG500X-24   00:00:55:00:66:66 1.3.5.34  Enabled Auto,         backup
      Native
3    ESW2-550X-48 00:24:98:75:45:00 6.2.10.11 Disabled Auto,slave slave
      Native
4    SG500X-24P   00:44:ff:44:33:ab 1.3.5.34  Disabled Auto,         slave
      Native

Topology is Ring

Stack image auto synchronization is enabled
```

<table>
<thead>
<tr>
<th>No.</th>
<th>Unit</th>
<th>Stack Port #1 Connected Operational Port</th>
<th>Stack Port #2 Connected Operational Port</th>
<th>After Reboot Stack Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SG500X-48P</td>
<td>00:00:44:55:66:77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SG500X-24</td>
<td>00:00:55:00:66:66</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ESW2-550X-48</td>
<td>00:24:98:75:45:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SG500X-24P</td>
<td>00:44:ff:44:33:ab</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Example 2—Show 1 unit in stack.**

```
switch000000# sh stack 1
Current stack mode is : advanced-hybrid-XG
MAC address: 00:00:b0:01:00:04
Master: Enabled
Unit number after reset: 1
Unit mode after reset: Advanced-Hybrid-XG
Status: master
Active image: imagel
Selected for next boot: imagel
Topology is Chain
Stack image auto synchronization is enabled
```

<table>
<thead>
<tr>
<th>Unit</th>
<th>Stack Port #1</th>
<th>Stack Port #2</th>
<th>After Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Port Speed</td>
<td>Unit Speed</td>
<td>Ports</td>
</tr>
<tr>
<td></td>
<td>S1-XG 3G</td>
<td>S2-XG 4G</td>
<td>S1-S2-Xg 1G</td>
</tr>
</tbody>
</table>

**Example 3—Show stack on Sx500 device.**

```
Current stack mode is : native
```

<table>
<thead>
<tr>
<th>Unit</th>
<th>Model Name</th>
<th>MAC Address</th>
<th>Software</th>
<th>Master</th>
<th>Unit No./Mode After Reboot</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SF500-24</td>
<td>00:24:05:11:08:49</td>
<td>1.3.5.34</td>
<td>Enabled</td>
<td>Auto, Native</td>
<td>master</td>
</tr>
<tr>
<td>2</td>
<td>SG500-28P</td>
<td>00:31:06:13:16:11</td>
<td>1.3.5.34</td>
<td>Enabled</td>
<td>Auto, Native</td>
<td>backup</td>
</tr>
<tr>
<td>3</td>
<td>SF500-48P</td>
<td>00:77:66:00:00:00</td>
<td>1.3.5.34</td>
<td>Disabled</td>
<td>Auto, Slave</td>
<td>slave</td>
</tr>
</tbody>
</table>
Native

Topology is Chain

Stack image auto synchronization is enabled

<table>
<thead>
<tr>
<th>Unit</th>
<th>Stack Port #1</th>
<th>Stack Port #2</th>
<th>After Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Port</th>
<th>Connected Operational Port</th>
<th>Speed</th>
<th>Connected Operational Port</th>
<th>Speed</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S3</td>
<td>2</td>
<td>1G</td>
<td>S4</td>
<td>link down</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>S3</td>
<td>1</td>
<td>1G</td>
<td>S4</td>
<td>3</td>
<td>1G</td>
</tr>
<tr>
<td>3</td>
<td>S3</td>
<td>2</td>
<td>1G</td>
<td>S4</td>
<td>link down</td>
<td>Down</td>
</tr>
</tbody>
</table>

8.15 switch renumber

Use the switch renumber Global Configuration command to change the unit ID of a specific unit.

**Syntax**

```
switch current-unit-id renumber new-unit-id
```

**Parameters**

- `current-unit-id`—Specify Unit number. (Range: 1–8)
- `new-unit-id`—The new unit number. (Range: 1–8, unit-id-auto)

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**User Guidelines**

This command takes place after reboot.
Example

The following renumbers unit 1 to unit 2.

```
switchxxxxxx# configure
switchxxxxxx(config)# switch 1 renumber 2
```
9.1 clock set

The clock set Privileged EXEC mode command manually sets the system clock.

Syntax

clock set hh:mm:ss [[day month] | [month day]] year

Parameters

- **hh:mm:ss**—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- **day**—Specifies the current day of the month. (Range: 1-31)
- **month**—Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- **year**—Specifies the current year. (Range: 2000–2037)

Command Mode

Privileged EXEC mode

User Guidelines

It is recommended that the user enter the local clock time and date.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
switchxxxxxx# clock set 13:32:00 7 Mar 2005
```

9.2 clock source

The clock source Global Configuration mode command configures an external time source for the system clock. Use the no form of this command to disable the external time source.
Syntax

```
clock source {sntp | browser}
no clock source
```

Parameters

- `sntp`—Specifies that an SNTP server is the external clock source.
- `browser`—Specifies that if the system clock is not already set (either manually or by SNTP) and a user login to the device using a WEB browser (either via HTTP or HTTPS), the system clock will be set according to the browser’s time information.

Default Configuration

There is no external clock source.

If no parameter is specified, SNTP will be configured as the time source.

If the command is executed twice, each time with a different clock source, both sources will be operational, SNTP has higher priority than time from browser.

Command Mode

Global Configuration mode

Example

The following example configures an SNTP server as an external time source for the system clock.

```
switchxxxxxx(config)# clock source sntp
switchxxxxxx(config)# clock source browser
switchxxxxxx(config)# exit
switchxxxxxx# show clock
*10:46:48 UTC May 28 2013
Time source is sntp
Time from Browser is enabled
```
### 9.3 clock timezone

Use the `clock timezone` Global Configuration command to set the time zone for display purposes. Use the `no` form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

**Syntax**

```
clock timezone zone hours-offset [minutes-offset]
no clock timezone
```

**Parameters**

- **zone**—The acronym of the time zone. (Range: Up to 4 characters)
- **hours-offset**—Hours difference from UTC. (Range: (-12)–(+13))
- **minutes-offset**—Minutes difference from UTC. (Range: 0–59)

**Default Configuration**

Offsets are 0.

Acronym is empty.

**Command Mode**

Global Configuration mode

**User Guidelines**

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

**Example**

```
switchxxxxxx(config)# clock timezone abc +2 minutes 32
```

---

### 9.4 clock summer-time

Use one of the formats of the `clock summer-time` Global Configuration command to configure the system to automatically switch to summer time (Daylight Saving Time). Use the `no` form of this command to configure the software not to automatically switch to summer time.
Syntax

```
clock summer-time zone recurring [usa | eu | {week day month hh:mm week day month hh:mm}] [offset]
clock summer-time zone date day month year hh:mm date month year hh:mm [offset]
clock summer-time zone date month day year hh:mm month day year hh:mm [offset]
no clock summer-time
```

Parameters

- **zone**—The acronym of the time zone to be displayed when summer time is in effect. (Range: up to 4 characters)
- **recurring**—Indicates that summer time starts and ends on the corresponding specified days every year.
- **date**—Indicates that summer time starts on the first date listed in the command and ends on the second date in the command.
- **usa**—The summer time rules are the United States rules.
- **eu**—The summer time rules are the European Union rules.
- **week**—Week of the month. Can be 1–5, first to last.
- **day**—Day of the week (first three characters by name, such as Sun).
- **date**—Date of the month. (Range: 1–31)
- **month**—Month (first three characters by name, such as Feb).
- **year**—Year (no abbreviation). (Range: 2000–2097)
- **hh:mm**—Time (military format) in hours and minutes. (Range: hh:mm hh: 0-23, mm: 0-59)
- **offset**—Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

Summer time is disabled.
Command Mode

Global Configuration mode

User Guidelines

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rules for Daylight Saving Time:

- **From 2007:**
  - **Start:** Second Sunday in March
  - **End:** First Sunday in November
  - **Time:** 2 AM local time

- **Before 2007:**
  - **Start:** First Sunday in April
  - **End:** Last Sunday in October
  - **Time:** 2 AM local time

EU rules for Daylight Saving Time:

- **Start:** Last Sunday in March
- **End:** Last Sunday in October
- **Time:** 1:00 am (01:00) Greenwich Mean Time (GMT)

Example

```
switchxxxxxx(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010 09:00
```

9.5 **clock dhcp timezone**

Use the `clock dhcp timezone` Global Configuration command to specify that the timezone and the Summer Time (Daylight Saving Time) of the system can be taken
from the DHCP Timezone option. Use the no form of this command disable this option.

Syntax

clock dhcp timezone

no clock dhcp timezone

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The TimeZone taken from the DHCP server has precedence over the static TimeZone.

The Summer Time taken from the DHCP server has precedence over static SummerTime.

The TimeZone and SummerTime remain effective after the IP address lease time has expired.

The TimeZone and SummerTime that are taken from the DHCP server are cleared after reboot.

The no form of the command clears the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the following precedence is applied:

- information received from DHCPv6 precedes information received from DHCPv4

- information received from DHCP client running on lower interface precedes information received from DHCP client running on higher interfac

Disabling the DHCP client from where the DHCP-TimeZone option was taken, clears the dynamic Time Zone and Summer Time configuration.
Example

switchxxxxxx(config)# clock dhcp timezone

9.6 sntp authentication-key

The sntp authentication-key Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the no form of this command to remove the authentication key for SNTP.

Syntax

```plaintext
sntp authentication-key key-number md5 key-value
encrypted sntp authentication-key key-number md5 encrypted-key-value
no sntp authentication-key key-number
```

Parameters

- **key-number**—Specifies the key number. (Range: 1–4294967295)
- **key-value**—Specifies the key value. (Length: 1–8 characters)
- **encrypted-key-value**—Specifies the key value in encrypted format.

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

Examples

The following example defines the authentication key for SNTP.

```plaintext
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp authenticate
```
9.7  sntp authenticate

The sntp authenticate Global Configuration mode command enables authentication for received SNTP traffic from servers. Use the no form of this command to disable the feature.

Syntax

sntp authenticate

no sntp authenticate

Parameters

N/A

Default Configuration

Authentication is disabled.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Examples

The following example enables authentication for received SNTP traffic and sets the key and encryption key.

```
switchxxxxxx(config)# sntp authenticate
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
```

9.8  sntp trusted-key

The sntp trusted-key Global Configuration mode command authenticates the identity of the system with which SNTP synchronizes. Use the no form of this command to disable system identity authentication.
Clock Commands

Syntax

sntp trusted-key key-number
no sntp trusted-key key-number

Parameters

key-number—Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both received unicast and broadcast.

Examples

The following example authenticates key 8.

switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate

9.9 sntp broadcast client enable

The sntp broadcast client enable Global Configuration mode command enables SNTP Broadcast clients.

Use the no form of this command to disable SNTP Broadcast clients.

Syntax

sntp broadcast client enable [both | ipv4 | ipv6]
no sntp broadcast client enable
Parameters

both—Specifies the IPv4 and IPv6 SNTP Broadcast clients are enabled. If the parameter is not defined it is the default value.

ipv4—Specifies the IPv4 SNTP Broadcast clients are enabled.

ipv6—Specifies the IPv6 SNTP Broadcast clients are enabled.

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp broadcast client enable` Interface Configuration mode command to enable the SNTP Broadcast client on a specific interface.

After entering this command, you must enter `clock source snmp` for the command to be run. If this command is not run, the switch will not synchronize with Broadcast servers.

Example

The following example enables SNTP Broadcast clients.

```
switchxxxxxx(config)# sntp broadcast client enable
```

9.10 sntp anycast client enable

The `sntp anycast client enable` Global Configuration mode command enables the SNTP Anycast client. Use the `no` form of this command to disable the SNTP Anycast client.

Syntax

`sntp anycast client enable [both | ipv4 | ipv6]`

`no sntp anycast client enable`

Parameters
• **both**—Specifies the IPv4 and IPv6 SNTP Anycast clients are enabled. If the parameter is not defined it is the default value.
• **ipv4**—Specifies the IPv4 SNTP Anycast clients are enabled.
• **ipv6**—Specifies the IPv6 SNTP Anycast clients are enabled.

**Default Configuration**
The SNTP anycast client is disabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
Use this command to enable the SNTP Anycast client.

**Example**
The following example enables SNTP Anycast clients.

```
switchxxxxxx(config)# sntp anycast client enable
```

9.11 **sntp client enable**
The **sntp client enable** Global Configuration mode command enables the SNTP Broadcast and Anycast client on an interface when the device is in Router mode (Layer 3). Use the **no** form of this command to disable the SNTP Broadcast and Anycast client.

**Syntax**
```
sntp client enable {interface-id}
no sntp client enable {interface-id}
```

**Parameters**
- **interface-id**—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

**Default Configuration**
The SNTP client is disabled on an interface.
Command Mode
Global Configuration mode - Ethernet port, Port-channel or VLAN.

User Guidelines
This command only works when the device is in Router mode (Layer 3).
The sntp broadcast client enable Global Configuration mode command globally enables Broadcast clients.
This command enables both.

Example
The following example enables the SNTP Broadcast and Anycast client on port gi1/1/3.

```
switchxxxxxx(config)# sntp client enable gi1/1/3
```

9.12 sntp client enable (Interface)
To enable the SNTP Broadcast and Anycast client on an interface, use the sntp client enable Interface Configuration command. Use the no form of this command to disable the SNTP client.
This command enables the SNTP Broadcast and Anycast client on an interface. Use the no form of this command to disable the SNTP client.

Syntax
```
sntp client enable
no sntp client enable
```

Parameters
N/A

Default Configuration
The SNTP client is disabled on an interface.

Command Mode
Interface Configuration (Ethernet, Port-channel, VLAN) mode
User Guidelines

The `sntp broadcast client enable` Global Configuration mode command globally enables Broadcast clients.

Example

The following example enables the SNTP broadcast and anycast client on an interface.

```
switchxxxxx(config-if)# sntp client enable
```

9.13 `sntp unicast client enable`

The `sntp unicast client enable` Global Configuration mode command enables the device to use Simple Network Time Protocol (SNTP)-predefined Unicast clients. Use the `no` form of this command to disable the SNTP Unicast clients.

Syntax

```
sntp unicast client enable
no sntp unicast client enable
```

Parameters

N/A

Default Configuration

The SNTP unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp server` Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use SNTP Unicast clients.

```
switchxxxxx(config)# sntp unicast client enable
```
### 9.14 sntp unicast client poll

The `sntp unicast client poll` Global Configuration mode command enables polling for the SNTP predefined Unicast clients. Use the `no` form of this command to disable the polling for the SNTP client.

**Syntax**

```plaintext
sntp unicast client poll
no sntp unicast client poll
```

**Default Configuration**

Polling is disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables polling for SNTP predefined unicast clients.

```
switchxxxxxx(config)# sntp unicast client poll
```

### 9.15 sntp server

The `sntp server` Global Configuration mode command configures the device to use the SNTP to request and accept Network Time Protocol (NTP) traffic from a specified server (meaning to accept system time from an SNTP server). Use the `no` form of this command to remove a server from the list of SNTP servers.

**Syntax**

```plaintext
sntp server {ip-address | hostname} [poll] [key keyid]
no sntp server {ip-address | hostname}
```

**Parameters**

- **ip-address**—Specifies the server IP address. This can be an IPv4, IPv6 or IPv6z address. See [IPv6z Address Conventions](#):
Clock Commands

- **hostname**—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length for each part of the hostname: 63 characters)

- **poll**—Enables polling.

- **key keyid**—Specifies the Authentication key to use when sending packets to this peer. (Range: 1–4294967295)

**Default Configuration**

No servers are defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Up to 8 SNTP servers can be defined.

The `sntp unicast client enable` Global Configuration mode command enables predefined Unicast clients.

The `sntp broadcast client enable` Global Configuration mode command globally enables Broadcast clients.

**Example**

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1 with polling.

```
switchxxxxxx(config)# sntp server 192.1.1.1 poll
```

9.16 **sntp source-interface**

Use the `sntp source-interface` Global Configuration mode command to specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SNTP servers. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
sntp source-interface interface-id
no sntp source-interface
```
Parameters

interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

The outgoing interface is selected based on the SNTP server's IP address. If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SNTP server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sntp source-interface vlan 10
```
Parameters

\textit{interface-id}—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

The outgoing interface is selected based on the SNTP server's IP address. If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SNTP server.

Example

The following example configures the VLAN 10 as the source interface.

\begin{verbatim}
switchxxxxxx(config)# sntp source-interface-ipv6 vlan 10
\end{verbatim}

9.18 \textbf{show clock}

The \texttt{show clock} EXEC mode command displays the time and date from the system clock.

Syntax

\texttt{show clock [detail]}

Parameters

detail—Displays the time zone and summer time configuration.
Command Mode
EXEC mode

Examples
Example 1 - The following example displays the system time and date.

```
switchxxxxxx# show clock
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP
Time from Browser is enabled
```

Example 2 - The following example displays the system time and date along with the time zone and summer time configuration.

```
switchxxxxxx# show clock detail
Time source is sntp
Time from Browser is enabled
Time zone (DHCPv4 on VLAN1):
Acronym is RAIN
Offset is UTC+2
Time zone (Static):
Offset is UTC+0
Summertime (DHCPv4 on VLAN1):
Acronym is SUN
Recurring every year.
Begins at first Sunday of Apr at 02:00.
Ends at first Tuesday of Sep at 02:00.
Offset is 60 minutes.
Summertime (Static):
Acronym is GMT
Recurring every year.
```
Begins at first Sunday of Mar at 10:00.
Ends at first Sunday of Sep at 10:00.
Offset is 60 minutes.
DHCP timezone: Enabled

9.19 show sntp configuration

The `show sntp configuration` Privileged EXEC mode command displays the SNTP configuration on the device.

Syntax

`show sntp configuration`

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the device's current SNTP configuration.

```
switchxxxxxx# show sntp configuration
SNTP port : 123
Polling interval: 1024 seconds
MD5 Authentication Keys
-----------------------------
2   John123
3   Alice456
-----------------------------
Authentication is not required for synchronization.
```
No trusted keys
Unicast Clients: enabled
Unicast Clients Polling: enabled
Server: 1.1.1.121
  Polling: disabled
  Encryption Key: disabled
Server: 3001:1:1::1
  Polling: enabled
  Encryption Key: disabled
Server: dns_server.company.com
  Polling: enabled
  Encryption Key: disabled
Broadcast Clients: enabled for IPv4 and IPv6
Anycast Clients: disabled
No Broadcast Interfaces
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10

9.20 show sntp status

The show sntp status Privileged EXEC mode command displays the SNTP servers status.

Syntax
show sntp status

Parameters
N/A

Default Configuration
N/A
Command Mode

Privileged EXEC mode

Example

The following example displays the SNTP servers status:

switchxxxxxx# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server: 176.1.1.8
   Source: DHCPv4 on VLAN 1
   Status: Up
   Last response: 19:58:22.289 PDT Feb 19 2005
   Stratum Level: 1
   Offset: 7.33mSec
   Delay: 117.79mSec
Server: dns_server.company.com
   Source: static
   Status: Unknown
   Last response: 12:17.17.987 PDT Feb 19 2005
   Stratum Level: 1
   Offset: 8.98mSec
   Delay: 189.19mSec
Server: 3001::1::1
   Source: DHCPv6 on VLAN 2
   Status: Unknown
   Last response:
   Offset: mSec
   Delay: mSec
Server: dns1.company.com
   Source: DHCPv6 on VLAN 20
   Status: Unknown
   Last response:
   Offset: mSec
   Delay: mSec

Anycast servers:
Server: 176.1.11.8
   Interface: VLAN 112
Status: Up
Stratum Level: 10
Offset: 9.98mSec
Delay: 289.19mSec
Broadcast servers:
Server: 3001:1::12
  Interface: VLAN 101
Stratum Level: 255
10.1 clear host

Use the clear host command in privileged EXEC mode to delete dynamic hostname-to-address mapping entries from the DNS client name-to-address cache.

**Syntax**

clear host {hostname | *}

**Parameters**

- **hostname**— Name of the host for which hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.
- **/***— Specifies that all the dynamic hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.

**Default Configuration**

No hostname-to-address mapping entries are deleted from the DNS client name-to-address cache.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

To remove the dynamic entry that provides mapping information for a single hostname, use the *hostname* argument. To remove all the dynamic entries, use the * keyword.

To define a static hostname-to-address mappings in the DNS hostname cache, use the ip host command.

To delete a static hostname-to-address mappings in the DNS hostname cache, use the no ip host command.
Example
The following example deletes all dynamic entries from the DNS client name-to-address cache.

```
clear host *
```

10.2  ip domain lookup
Use the ip domain lookup command in Global Configuration mode to enable the IP Domain Naming System (DNS)-based host name-to-address translation.

To disable the DNS, use the no form of this command.

Syntax
```
ip domain lookup
no ip domain lookup
```

Parameters
N/A

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
The following example enables DNS-based host name-to-address translation.

```
switchxxxxxx(config)# ip domain lookup
```

10.3  ip domain name
Use the ip domain name command in Global Configuration mode, to define a default domain name that the switch uses to complete unqualified hostnames (names without a dotted-decimal domain name).
To delete the static defined default domain name, use the **no** form of this command.

**Syntax**

`ip domain name name`

`no ip domain name`

**Parameters**

`name`— Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. Length: 1–158 characters. Maximum label length of each domain level is 63 characters.

**Default Configuration**

No default domain name is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and the default domain name appended to it before being added to the host table.

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of each domain level is 63 characters. The maximum name size is 158 bytes.

**Example**

The following example defines the default domain name as ‘www.website.com’.

```
switchxxxxxx(config)# ip domain name website.com
```
10.4 ip domain polling-interval

Use the ip domain polling-interval command in Global Configuration mode to specify the polling interval.

Use the no form of this command to return to the default behavior.

**Syntax**

```plaintext
ip domain polling-interval seconds
no ip domain polling-interval
```

**Parameters**

- `seconds`— Polling interval in seconds. The range is from \((2 \times (R+1) \times T)\) to 3600.

**Default Configuration**

The default value is \(2 \times (R+1) \times T\), where

- \(R\) is a value configured by the ip domain retry command.
- \(T\) is a value configured by the ip domain timeout command.

**Command Mode**

Global Configuration mode

**User Guidelines**

Some applications communicate with the given IP address continuously. DNS clients for such applications, which have not received resolution of the IP address or have not detected a DNS server using a fixed number of retransmissions, return an error to the application and continue to send DNS Request messages for the IP address using the polling interval.

**Example**

The following example shows how to configure the polling interval of 100 seconds:

```plaintext
ip domain polling-interval 100
```
10.5  ip domain retry

Use the `ip domain retry` command in Global Configuration mode to specify the number of times the device will send Domain Name System (DNS) queries when there is no replay.

To return to the default behavior, use the `no` form of this command.

Syntax

```
ip domain retry number
no ip domain retry
```

Parameters

- `number`—Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 16.

Default Configuration

The default value is 1.

Command Mode

Global Configuration mode

User Guidelines

The number argument specifies how many times the DNS query will be sent to a DNS server until the switch decides that the DNS server does not exist.

Example

The following example shows how to configure the switch to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

10.6  ip domain timeout

Use the `ip domain timeout` command in Global Configuration mode to specify the amount of time to wait for a response to a DNS query.

To return to the default behavior, use the `no` form of this command.
**Syntax**

`ip domain timeout seconds`

`no ip domain timeout`

**Parameters**

`seconds`— Time, in seconds, to wait for a response to a DNS query. The range is from 1 to 60.

**Default Configuration**

The default value is 2 seconds.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the command to change the default time out value. Use the `no` form of this command to return to the default time out value.

**Example**

The following example shows how to configure the switch to wait 50 seconds for a response to a DNS query:

```
ip domain timeout 50
```

10.7 **ip host**

Use the `ip host` Global Configuration mode command to define the static host name-to-address mapping in the DNS host name cache.

Use the `no` form of this command to remove the static host name-to-address mapping.

**Syntax**

`ip host hostname address1 [address2...address8]`

`no ip host name ip host name [address1...address8]`
Parameters

- **hostname**— Name of the host. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters).
- **address1**— Associated host IP address (IPv4 or IPv6, if IPv6 stack is supported).
- **address2...address8**— Up to seven additional associated IP addresses, delimited by a single space (IPv4 or IPv6, if IPv6 stack is supported).

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

An IP application will receive the IP addresses in the following order:

1. IPv6 addresses in the order specified by the command.
2. IPv4 addresses in the order specified by the command.

Use the no format of the command with the address1...address8 argument to delete the specified addresses. The entry is deleted if all its addresses are deleted.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
ip host accounting.website.com 176.10.23.1
```

10.8 **ip name-server**

Use the ip name-server command in Global Configuration mode to specify the address of one or more name servers to use for name and address resolution.
Use the **no** form of this command to remove the static specified addresses.

**Syntax**

```plaintext
ip name-server server1-address [server-address2...server-address8]
no ip name-server [server-address1...server-address8]
```

**Parameters**

- `server-address1`—IPv4 or IPv6 addresses of a single name server.
- `server-address2...server-address8`—IPv4 or IPv6 addresses of additional name servers.

**Default Configuration**

No name server IP addresses are defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

The preference of the servers is determined by the order in which they were entered.

Each `ip name-server` command replaces the configuration defined by the previous one (if one existed).

**Example**

The following example shows how to specify IPv4 hosts 172.16.1.111, 172.16.1.2, and IPv6 host 2001:0DB8::3 as the name servers:

```plaintext
ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

### 10.9 **show hosts**

Use the `show hosts` command in privileged EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
**Syntax**

```plaintext
show hosts [all | hostname]
```

**Parameters**

- **all**—The specified host name cache information is to be displayed for all configured DNS views. This is the default.
- **hostname**—The specified host name cache information displayed is to be limited to entries for a particular host name.

**Command Mode**

Privileged EXEC

**Default Configuration**

Default is `all`.

**User Guidelines**

This command displays the default domain name, a list of name server hosts, and the cached list of host names and addresses.

**Example**

The following is sample output with no parameters specified:

```plaintext
show hosts
Name/address lookup is enabled
Domain Timeout: 3 seconds
Domain Retry: 4 times
Domain Polling Interval: 10 seconds

Default Domain Table
Source  Interface Preference Domain
static                      website.com
dhcpv6  vlan 100   1      qqtca.com
dhcpv6  vlan 100   2      company.com
dhcpv6  vlan 1100  1      pptca.com
```
**Name Server Table**

<table>
<thead>
<tr>
<th>Source</th>
<th>Interface</th>
<th>Preference</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td></td>
<td>1</td>
<td>192.0.2.204</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td>2</td>
<td>192.0.2.205</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td>3</td>
<td>192.0.2.105</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>vlan 100</td>
<td>1</td>
<td>2002:0:22AC::11:231A:0BB4</td>
</tr>
<tr>
<td>DHCPv4</td>
<td>vlan 1</td>
<td>1</td>
<td>192.1.122.20</td>
</tr>
<tr>
<td>DHCPv4</td>
<td>vlan 1</td>
<td>2</td>
<td>154.1.122.20</td>
</tr>
</tbody>
</table>

**Cache Table**

Flags: (static/dynamic, OK/Ne/??)

OK - Okay, Ne - Negative Cache, ?? - No Response

Host Flag Address; Age...in preference order

- example1.company.com (dynamic, OK) 2002:0:130F::0A0:1504:0BB4;1 112.0.2.10 176.16.8.8;123 124 173.0.2.30;39
- example2.company.com (dynamic, ??)
- example3.company.com (static, OK) 120.0.2.27
- example4.company.com (dynamic, OK) 24 173.0.2.30;15
- example5.company.com (dynamic, Ne); 12
11.1 copy

The copy Privileged EXEC mode command copies a source file to a destination file.

Syntax

copy source-url destination-url [exclude | include-encrypted | include-plaintext]

Parameters

- source-url—Specifies the source file URL or source file reserved keyword to be copied. (Length: 1–160 characters)
- destination-url—Specifies the destination file URL or destination file reserved keyword. (Length: 1–160 characters).
- "Flash://" —The source or destination URL scheme that specifies the access method to the local flash memory. It stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-config).
- exclude—Do not include sensitive data in the file being copied.
- include-encrypted—Include sensitive data in its encrypted form.
- include-plaintext—Include sensitive data in its plaintext form

The following table displays the URL options.

<table>
<thead>
<tr>
<th>Source and/or Destination URL</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config</td>
<td>Currently running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>flash://startup-config</td>
<td></td>
</tr>
<tr>
<td>image</td>
<td>Image file. If specified as the source file, it is the active image file. If specified as the destination file, it is the non-active image file.</td>
</tr>
<tr>
<td>flash://image</td>
<td></td>
</tr>
<tr>
<td>boot</td>
<td>Boot file.</td>
</tr>
<tr>
<td>Source and/or Destination URL</td>
<td>Source or Destination</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>tftp://</strong></td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is <code>tftp://host/[directory]/filename</code>. The host can be either an IP address or a host name.</td>
</tr>
<tr>
<td><strong>scp</strong></td>
<td>Source or destination URL for a Secure Copy Protocol (SCP) network server. The syntax for this alias is: <code>scp://[username,password@]host/[directory]/filename</code>. The host can be either the IP address or hostname. The default on the switch is SSH authentication by password with username and password <code>anonymous</code>. The SSH authentication parameters can be reconfigured to match the SSH/SCP server’s parameters.</td>
</tr>
<tr>
<td><strong>xmodem:</strong></td>
<td>Source for the file from a serial connection that uses the Xmodem protocol.</td>
</tr>
<tr>
<td><strong>unit://member/image</strong></td>
<td>Image file on one of the units. To copy from the master to all units, specify <code>*</code> in the member field.</td>
</tr>
<tr>
<td><strong>unit://member/boot</strong></td>
<td>Boot file on one of the units. To copy from the master to all units, specify <code>*</code> in the member field.</td>
</tr>
<tr>
<td><strong>unit://member/startup-config</strong></td>
<td>Configuration file used during initialization (startup) on one of the units.</td>
</tr>
<tr>
<td><strong>null:</strong></td>
<td>Null destination for copies or files. A remote file can be copied to null to determine its size. For instance <code>copy running-conf null</code> returns the size of the running configuration file.</td>
</tr>
<tr>
<td><strong>backup-config</strong></td>
<td>Backup configuration file. A configuration file can be downloaded to this file (without giving a file name). This can then be copied to the running-conf or startup-conf files.</td>
</tr>
<tr>
<td><strong>unit://member/backup-config</strong></td>
<td>Backup configuration file on one of the units.</td>
</tr>
<tr>
<td><strong>mirror-config</strong></td>
<td>Mirrored configuration file. If the running config and the startup config have been identical for 24 hours, the startup config is automatically copied to the mirror-conf file by the system. It can then be copied to the startup or running conf if required.</td>
</tr>
<tr>
<td><strong>localization</strong></td>
<td>This enables copying a language dictionary file to the secondary language file, such as in <code>copy tftp://10.5.234.203/french.txt localization</code>. This creates French as the second language. the file <code>french.txt</code> is the French dictionary.</td>
</tr>
<tr>
<td><strong>unit://member/localization</strong></td>
<td>The secondary language file on one of the units. To copy to all units, specify <code>*</code> in the member field. Example: <code>copy tftp://10.5.234.203/french.txt unit:// */localization</code>.</td>
</tr>
</tbody>
</table>
Default Configuration
Sensitive data is excluded if no method was specified

Command Mode
Privileged EXEC mode

User Guidelines
The location of the file system dictates the format of the source or destination URL.
The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

IPv6z Address Format
If the IPv6 address is a Link Local address (IPv6z address), the outgoing interface name must be specified. The format of an IPv6z address is: {ipv6-link-local-address}%{interface-id}. The subparameters are:

- ipv6-link-local-address—Specifies the IPv6 Link Local address.
- interface-id—{<port-type>[ ]<port-number>}{port-channel | po}{<port-channel-number> | {tunnel | tu}{<tunnel-number> | vlan}[ ]<vlan-id>

If the egress interface is not specified, the default interface is selected. The following combinations are possible:

- ipv6_address%interface_id - Refers to the IPv6 address on the interface specified.
- ipv6_address%0 - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- ipv6_address - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

Invalid Combinations of Source and Destination
The following are invalid combinations of source and destination files:

- The source file and destination file are the same file.

<table>
<thead>
<tr>
<th>Source and/or Destination URL</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging</td>
<td>Specifies the SYSLOG file.</td>
</tr>
<tr>
<td>Word&lt;1-128&gt;</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>
• **xmodem**: is the destination file. The source file can be copied to **image**, **boot** and **null**: only.

• **tftp://**: is the source file and destination file on the same copy.

• ***.prv** files cannot be copied. The source or destination is a slave unit (except for image and boot files).

• **mirror-config** cannot be used as a destination

The following table describes the characters displayed by the system when **copy** is being run:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).</td>
</tr>
<tr>
<td>.</td>
<td>For network transfers, indicates that the copy process timed out.</td>
</tr>
</tbody>
</table>

**Various Copy Options Guidelines**

- **Copying an Image File from a Server to Flash Memory**

  Use the `copy source-url flash://image` command to copy an image file from a server to flash memory. When the administrator copies an image file from the server to a device, the image file is saved to the “inactive” image. To use this image, the administrator must switch the inactive image to the active image and reboot. The device will then use this new image.

- **Copying a Boot File from a Server to Flash Memory**

  Use the `copy source-url boot` command to copy a boot file from a server to flash memory. **Copying a Configuration File from a Server to the Running Configuration File**

  Use the `copy source-url running-config` command to load a configuration file from a network server to the running configuration file of the device. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration files, with the loaded configuration file taking precedence.

- **Copying a Configuration File from a Server to the Startup Configuration**
Use the `copy source-url startup-config` command to copy a configuration file from a network server to the device startup configuration file. The startup configuration file is replaced by the copied configuration file.

- **Storing the Running Config or Startup Config on a Server**
  Use the `copy running-config destination-url` command to copy the current configuration file to a network server using TFTP.
  Use the `copy startup-config destination-url` command to copy the startup configuration file to a network server.

- **Saving the Running Configuration to the Startup Configuration**
  Use the `copy running-config startup-config` command to copy the running configuration to the startup configuration file.

- **Backing Up the Running Configuration or Startup Configuration to the Backup Configuration**
  Use the `copy running-config backup-config` command to back up the running configuration to the backup configuration file.
  Use the `copy startup-config backup-config` command to back up the startup configuration to the backup configuration file.

- **Restoring the Mirror Configuration File.**
  Use `copy mirror-config startup-config` or `copy mirror-config running-config` to copy the mirror configuration file to one of the configuration files being used.

### SCP Copy Authentication Options

The following options are possible for using the SCP copy feature:

- **scp://host/[directory]/filename**
  In this option, the SSH authentication method (either by password or by key) and the credentials are specified by the CLI commands for `ip ssh client authentication`, `ip ssh-client key-type` or `ip ssh-client password/username`, and also the server authentication configuration commands.

- **scp://username,password@host/[directory]/filename.**
  This option specifies SSH authentication by password, and the user name and password for this specific SCP session (one-time only).
Examples

**Example 1** - The following example copies system image file1 from the TFTP server 172.16.101.101 to the non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

**Example 2** - Copying an Image from a Server to Flash Memory

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

**Example 3** - Copying the mirror-config file to the startup-configuration file

The following example copies the mirror configuration file, saved by the system, to the Startup Configuration file.

```
switchxxxxxx# copy mirror-config startup-config
```

**Example 4** - Copy file1 from SCP server to startup config
The following example copies file1 to the Startup Configuration file. The username and password used for SCP session authentication are: jeff and admin1. The IP address of the server containing file1 is 102.1.2.2.

```
switchxxxxxx# copy scp://jeff:admin1@102.1.2.2/file1 startup-config
```
11.2 write memory

Use the **write memory** Privileged EXEC mode command to save the Running Configuration file to the Startup Configuration file.

**Syntax**

```
write memory
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Examples**

This example shows how to overwrite the startup-config with the running-config.

```
switchxxxxxx# write memory
15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
```
11.3 write

Use the **write** Privileged EXEC mode command to save the running configuration to the startup configuration file.

**Syntax**

`write [memory]`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Examples**

The following example shows how to overwrite the startup-config file with the running-config file with the `write` command.

```
switchxxxxxx# write
```

11.4 delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

**Syntax**

`delete url`
Parameters

url—Specifies the location URL or reserved keyword of the file to be deleted. (Length: 1–160 characters)

“Flash://” is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g., for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays keywords and URL prefixes:

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

mirror-config, *.sys, *.prv, image-1 and image-2 files cannot be deleted.

Example

The following example deletes the file called ‘backup-config’ from the flash memory.

```
switchxxxxx# delete flash://backup-config
Delete flash://backup-config? [confirm]
```

11.5 dir

The **dir** Privileged EXEC mode command displays the list of files on a flash file system.

Syntax

dir [directory-path]
Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

Example 1. The following example displays the list of files on a flash file system with static images. The Flash size column for all files except dynamic image specifies the maximum allowed size. The Data size column for dynamic images specifies the real size in the FLASH occupied by the file.

switchxxxxxxx# dir

Directory of flash:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Permission</th>
<th>Flash Size</th>
<th>Data Size</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>backuplo</td>
<td>rw</td>
<td>851760</td>
<td>525565</td>
<td>22-Dec-2010 10:50:32</td>
</tr>
<tr>
<td>backup-config</td>
<td>rw</td>
<td>524288</td>
<td>104</td>
<td>01-Jan-2010 05:35:04</td>
</tr>
<tr>
<td>image-1</td>
<td>rw</td>
<td>10485760</td>
<td>10485760</td>
<td>01-Jan-2010 06:10:23</td>
</tr>
<tr>
<td>image-2</td>
<td>rw</td>
<td>10485760</td>
<td>10485760</td>
<td>01-Jan-2010 05:43:54</td>
</tr>
<tr>
<td>mirror-config</td>
<td>rw</td>
<td>524288</td>
<td>104</td>
<td>01-Jan-2010 05:35:04</td>
</tr>
<tr>
<td>dhcpsn.prv</td>
<td>--</td>
<td>262144</td>
<td>--</td>
<td>01-Jan-2010 05:25:07</td>
</tr>
<tr>
<td>syslog1.sys</td>
<td>r-</td>
<td>524288</td>
<td>--</td>
<td>01-Jan-2010 05:57:00</td>
</tr>
<tr>
<td>syslog2.sys</td>
<td>r-</td>
<td>524288</td>
<td>--</td>
<td>01-Jan-2010 05:57:00</td>
</tr>
<tr>
<td>directory.prv</td>
<td>--</td>
<td>262144</td>
<td>--</td>
<td>01-Jan-2010 05:25:07</td>
</tr>
<tr>
<td>startup-config</td>
<td>rw</td>
<td>786432</td>
<td>1081</td>
<td>01-Jan-2010 10:05:34</td>
</tr>
</tbody>
</table>

Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes
11.6 more

The more Privileged EXEC mode command displays a file.

Syntax

more url

Parameters

url—Specifies the location URL or reserved keyword of the source file to be displayed. (Length: 1–160 characters).

“Flash://” is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays options for the URL parameter:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config</td>
<td>Current running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>mirror-config</td>
<td>Mirrored configuration file.</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

*.prv files cannot be displayed.

Example

The following example displays the running configuration file contents.

switchxxxxxx# more running-config
no spanning-tree
interface range gi1/1/1-48
speed 1000
exit
no lldp run
line console
exec-timeout 0

11.7 rename

The rename Privileged EXEC mode command renames a file.

Syntax

rename url new-url

Parameters

- url—Specifies the file location URL. (Length: 1–160 characters)
- new-url—Specifies the file's new URL. (Length: 1–160 characters)

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays options for the URL parameter:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;1-12</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
<tr>
<td>8&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

mirror-config, *.sys and *.prv files cannot be renamed.
Example
The following example renames the configuration backup file.

```
switchxxxxxx# rename backup-config m-config.bak
```

11.8 boot system
The `boot system` Privileged EXEC mode command specifies the active system image file that will be loaded by the device at startup.

Syntax
```
boot system {image-1 | image-2} [switch unit-id | all]
```

Parameters
- `switch unit-id`—Specifies the unit number.
- `all`—Specifies that the active image of all units is being set by the command.
- `image-1`—Specifies that image-1 is loaded as the system image during the next device startup.
- `image-2`—Specifies that image-2 is loaded as the system image during the next device startup.

Default Configuration
The default unit number is the master unit number (if the `switch` parameter is omitted, the active system image file that will be loaded by the device at startup will be set only for the master unit).

Command Mode
Privileged EXEC mode

User Guidelines
Use the `show bootvar` command to display the active image.
Example

The following example specifies that image-1 is the active system image file loaded by the device at startup. The results of this command is displayed in show bootvar.

```
switchxxxxxx# boot system image-1
switchxxxxxx# show bootvar
```

<table>
<thead>
<tr>
<th>Unit</th>
<th>Image</th>
<th>Filename</th>
<th>Version</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>image-1</td>
<td>1.2.0.34</td>
<td>04-Jul-2011</td>
<td>Not active*</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>image-2</td>
<td>1.2.0.38</td>
<td>13-Jul-2011</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>image-1</td>
<td>1.2.0.38</td>
<td>13-Jul-2011</td>
<td>Active*</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>image-2</td>
<td>1.2.0.34</td>
<td>04-Jul-2011</td>
<td>Not active</td>
</tr>
</tbody>
</table>

"*" designates that the image was selected for the next boot

11.9 show bootvar

Use the show bootvar EXEC mode command to display the active system image file that was loaded by the device at startup, and to display the system image file that will be loaded after rebooting the switch.

Syntax

```
show bootvar [unit unit-id]
```

Parameters

unit-id—Specifies the unit number. Range 1-8

Command Mode

EXEC mode
### Example

The following example displays the active system image file that was loaded by the device at startup and the system image file that will be loaded after rebooting the switch.

```plaintext
switchxxxxxx# show bootvar
```

<table>
<thead>
<tr>
<th>Unit</th>
<th>Image</th>
<th>filename</th>
<th>Version</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>file1</td>
<td>3.1.31</td>
<td>23-Jul-2002</td>
<td>Active</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>file2</td>
<td>3.2.19</td>
<td>22-Jan-2003</td>
<td>Not active*</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>file1</td>
<td>3.1.31</td>
<td>23-Jul-2002</td>
<td>Not active</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>file2</td>
<td>3.2.19</td>
<td>22-Jan-2003</td>
<td>Active</td>
</tr>
</tbody>
</table>

"*": Designates that the image was selected for the next boot.

### 11.10 show running-config

The `show running-config` Privileged EXEC mode command displays the entire current Running Configuration file contents or the contents of the file for the specified interface(s).

#### Syntax

```
show running-config [interface interface-id-list | detailed | brief]
```

#### Parameters

- `interface interface-id-list`—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.
- `detailed`—Displays configuration with SSL and SSH keys.
- `brief`—Displays configuration without SSL and SSH keys.

#### Default Configuration

All interfaces are displayed. If `detailed` or `brief` is not specified, the default is `detailed`.

#### Command Mode

Privileged EXEC mode
User Guidelines

Only non-default configurations are displayed.

Example

The following example displays the Running Configuration file contents.

Example 1 - Show the entire Running Configuration file.

```
switchxxxxxx# show running-config
no spanning-tree
interface range gi1/1/1-48
  speed 1000
  exit
no lldp run
interface vlan 1
  ip address 1.1.1.1 255.0.0.0
  exit
line console
  exec-timeout 0
  exit
switchxxxxxx#
```

Example 2 - Show the entire Running Configuration file for ports 1 and 2.

```
switchxxxxxx# show running-config interface gi1/1/1-2
interface gi1/1/1
  back-pressure
  duplex half
  speed 10
  flowcontrol on
  negotiation 10h 100h 100f
  dot1x max-req 8
  description "Hello World String"
```
lacp timeout short
lacp port-priority 1234
garp timer join 100
garp timer leave 300
port security max 111
port security mode max-addresses
spanning-tree disable
spanning-tree portfast auto
spanning-tree link-type point-to-point
spanning-tree cost 200000
spanning-tree port-priority 224
spanning-tree guard root
spanning-tree mst 2 port-priority 64
spanning-tree mst 2 cost 2222
spanning-tree mst 4 port-priority 80
qos cos 6
traffic-shape 12345
switchport mode general
switchport general allowed vlan add 12,14-20 tagged
switchport general allowed vlan add 2-11,13,100,3000,3002,3004,3006,3008 untagged
switchport general map macs-group 1 vlan 111
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
interface gi1/1/2
ip address 1.100.100.100 255.0.0.0
switchport mode trunk
switchport general map macs-group 1 vlan 111
switchport general map subnets-group 1 vlan 113
switchport general map protocols-group 1 vlan 112
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
switchport trunk native vlan 22

11.11 show startup-config

The show startup-config Privileged EXEC mode command displays the startup configuration file contents.

Syntax

show startup-config [interface interface-id-list]

Parameters

- interface interface-id-list—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.

Default Configuration

All interfaces are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

The Startup Configuration file does not contain all the information that can be displayed in the output. Only non-default configurations are displayed.

Examples

Example 1 - The following example displays the Startup Configuration file contents.

switchxxxxxx# show startup-config
no spanning-tree
interface range gi1/1/1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#

Example 2 - The following example displays the Startup Configuration file contents for ports 1 and 2.

switchxxxxxx# show startup-config interface gi1/1/1-2
interface gi1/1/1
back-pressure
duplex half
speed 10
flowcontrol on
negotiation 10h 100h 100f
dot1x max-req 8
description "Hello World String"
lacp timeout short
lacp port-priority 1234
garp timer join 100
garp timer leave 300
port security max 111
port security mode max-addresses
spanning-tree disable
spanning-tree portfast auto
spanning-tree link-type point-to-point
spanning-tree cost 200000
spanning-tree port-priority 224
spanning-tree guard root
spanning-tree mst 2 port-priority 64
spanning-tree mst 2 cost 2222
spanning-tree mst 4 port-priority 80
qos cos 6
traffic-shape 12345
switchport mode general
switchport general allowed vlan add 12,14-20 tagged
switchport general allowed vlan add 2-11,13,100,3000,3002,3004,3006,3008 untagged
switchport general map macs-group 1_vlan_111
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
interface gi1/1/2
ip address 1.100.100.100 255.0.0.0
switchport mode trunk
switchport general map macs-group 1_vlan_111
switchport general map subnets-group 1_vlan_113
switchport general map protocols-group 1_vlan_112
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
switchport trunk native vlan 22

11.12  service mirror-configuration

Use the service mirror-configuration Global Configuration mode command to enable the mirror-configuration service. Use no service mirror-configuration command to disable the service.
Syntax

service mirror-configuration

no service mirror-configuration

Parameters

- There are no parameters for this command

Default Configuration

The default configuration is mirror-configuration service enabled.

Command Mode

Global Configuration mode

User Guidelines

The mirror-configuration service automatically keeps a copy of the last known stable configuration (startup configuration that wasn't modified for 24H). The mirror-configuration file is not deleted when restoring to factory default.

When this service is disabled, the mirror-configuration file is not created and if such file already exists, it is deleted.

Note that enabling the service doesn't implicitly creates a mirror-configuration file.

Examples

1. The following example disables the mirror-configuration service

   no service mirror-configuration

   This operation will delete the mirror-config file if exists. Do you want to continue? (Y/N) [N]

2. The following example enables the mirror-configuration service

   service mirror-configuration

   Service is enabled.

   Note that the running-configuration must be first copied to the startup-configuration in order to initiate backing up the startup-config to the mirror-config.
11.13  show mirror-configuration service

Use the show mirror-configuration service EXEC mode command to display the mirror-configuration service status set by service mirror-configuration.

Syntax

show mirror-configuration service

Command Mode

EXEC mode

Example

The following example displays the status of the mirror-configuration service

show mirror-configuration service

Mirror-configuration service is enabled
12.1 boot host auto-config

Use the `boot host auto-config` Global Configuration mode command to enable DHCP auto configuration via either the TFTP or SCP protocols. Use the no form of this command to disable DHCP auto configuration.

**Syntax**

```plaintext
boot host auto-config [tftp | scp | auto [extension]]
no boot host auto-config
```

**Parameters**

- **tftp**: Only the TFTP protocol is used by auto-configuration.
- **scp**: Only the SCP protocol is used by auto-configuration.
- **auto** (Default) Auto-configuration uses the TFTP or SCP protocol depending on the configuration file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
  - **extension**: The SCP file extension. When no value is specified, 'scp' is used. (Range: 1–16 characters)

**Default Configuration**

The auto option is the default.

**Command Mode**

Global Configuration mode

**Default Configuration**

Enabled by default.

**Examples:**

Example 1. The following example specifies the auto mode and specifies "scon" as the SCP extension:

```plaintext
boot host auto-config auto scon
```
Example 2. The following example specifies the auto mode and does not provide an SCP extension. In this case "scp" is used.

```
boot host auto-config auto
```

Example 3. The following example specifies that only the SCP protocol will be used:

```
boot host auto-config scp
```

## 12.2 `show boot`

Use the `show boot` Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

### Syntax

```
show boot
```

### Parameters

N/A

### Default Configuration

N/A

### Command Mode

Privilege EXEC mode

### Examples

```
switchxxxxxx show boot
Auto Config

---------------
Config Download via DHCP: enabled
Download Protocol Mode is SCP
SCP extension is scp
Next Boot Config Download via DHCP: default
```
12.3 \textit{ip dhcp tftp-server ip address}

Use the \texttt{ip dhcp tftp-server ip address} Global Configuration mode command to set the TFTP or SCP server’s IP address. This address server as the default address used by a switch when it has not been received from the DHCP server. Use the no form of the command to return to default.

\textbf{Syntax}

\texttt{ip dhcp tftp-server ip address \textit{ip-addr}}

\texttt{no ip dhcp tftp-server ip address}

\textbf{Parameters}

\textit{ip-addr}— IPv4 Address or IPv6 Address or DNS name of TFTP or SCP server.

\textbf{Default Configuration}

No IP address

\textbf{Command Mode}

Global Configuration mode

\textbf{User Guidelines}

The backup server can be a TFTP server. It can also be an SCP server.

\textbf{Examples}

\textbf{Example 1.} The example specifies the IPv4 address of TFTP server:

```
switchxxxxxx(conf)# ip dhcp tftp-server ip address 10.5.234.232
```

\textbf{Example 2.} The example specifies the IPv6 address of TFTP server:

```
switchxxxxxx(conf)# ip dhcp tftp-server ip address 3000:1::12
```

\textbf{Example 3.} The example specifies the IPv6 address of TFTP server:
12.4  **ip dhcp tftp-server file**

Use the *ip dhcp tftp-server file* Global Configuration mode command to set the full file name of the configuration file to be downloaded on the TFTP or SCP server when it has not been received from the DHCP server. This serves as the default configuration file.

Use the no form of this command to remove the name.

**Syntax**

```
ip dhcp tftp-server file file-path
no ip dhcp tftp-server file
```

**Parameters**

- `file-path`—Full file path and name of the configuration file on the server

**Default Configuration**

No file name

**Command Mode**

Global Configuration mode

**Examples**

```
switchxxxxxx(conf)# ip dhcp tftp-server file conf/conf-file
```

12.5  **show ip dhcp tftp-server**

Use the *show ip dhcp tftp-server* EXEC mode command to display information about the TFTP/SCP server.

**Syntax**

```
show ip dhcp tftp-server
```

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC

Example

switchxxxxxx# show ip dhcp tftp-server
server address
active 1.1.1.1 from sname
manual 2.2.2.2
file path on tftp server
file path on server
active conf/conf-file from option 67
Management ACL Commands

13.1 management access-list

The management access-list Global Configuration mode command configures a management access list (ACL) and enters the Management Access-List Configuration command mode. Use the no form of this command to delete an ACL.

Syntax

management access-list name
no management access-list name

Parameters

name—Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-List Configuration mode, where the denied or permitted access conditions are defined with the deny and permit commands.

If no match criteria are defined, the default value is deny.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the management access-class command to select the active access list.

The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.
Example

Example 1 - The following example creates a management access list called mlist, configures management gi1/1/1 and gi1/1/9, and makes the new access list the active list.

```
switchxxxxxxx(config)# management access-list mlist
switchxxxxxxx(config-macl)# permit gi1/1/1
switchxxxxxxx(config-macl)# permit gi1/1/9
switchxxxxxxx(config-macl)# exit
switchxxxxxxx(config)# management access-class mlist
```

Example 2 - The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except gi1/1/1 and 9, and makes the new access list the active list.

```
switchxxxxxxx(config)# management access-list mlist
switchxxxxxxx(config-macl)# deny gi1/1/1
switchxxxxxxx(config-macl)# deny gi1/1/9
switchxxxxxxx(config-macl)# permit
switchxxxxxxx(config-macl)# exit
switchxxxxxxx(config)# management access-class mlist
```

13.2 permit (Management)

The permit Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).

Syntax

```
permit [interface-id] [service service]
permit ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]
```
Parameters

- **interface-id**:—Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN

- **service service** — Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.

- **ipv4-address**— Specifies the source IPv4 address.

- **ipv6-address/ipv6-prefix-length**— Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.

- **mask mask** — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.

- **mask prefix-length** — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the ACL called *mlist*

```plaintext
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

13.3 **deny (Management)**

The **deny** Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).
Syntax

deny [interface-id] [service service]

deny ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service service**—Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**—Specifies the source IPv4 address.
- **ipv6-address/ipv6-prefix-length**—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask mask**—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- **mask prefix-length**—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the ACL called mlist.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```
13.4 management access-class

The `management access-class` Global Configuration mode command restricts management connections by defining the active management access list (ACL). To disable management connection restrictions, use the `no` form of this command.

**Syntax**

```
management access-class {console-only | name}
no management access-class
```

**Parameters**

- **console-only**—Specifies that the device can be managed only from the console.
- **name**—Specifies the ACL name to be used. (Length: 1–32 characters)

**Default Configuration**

The default configuration is no management connection restrictions.

**Command Mode**

Global Configuration mode

**Example**

The following example defines an access list called `mlist` as the active management access list.

```
switchxxxxxx(config)# management access-class mlist
```

13.5 show management access-list

The `show management access-list` Privileged EXEC mode command displays management access lists (ACLs).

**Syntax**

```
show management access-list [name]
```
Parameters

name—Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the mlist management ACL.

```
switchxxxxxx# show management access-list mlist
ml
--
deny service telnet
permit gi1/1/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

### 13.6 show management access-class

The `show management access-class` Privileged EXEC mode command displays information about the active management access list (ACLs).

Syntax

```
show management access-class
```

Command Mode

Privileged EXEC mode
Example
The following example displays the active management ACL information.

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```
14.1 snmp-server server

Use the `snmp-server server` Global Configuration mode command to enable the device to be configured by the SNMP protocol. Use the `no` form of this command to disable this function.

**Syntax**

```
snmp-server server
no snmp-server server
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxxx(config)# snmp-server server
```

14.2 snmp-server community

Use the `snmp-server community` Global Configuration mode command to set the community access string (password) that permits access to SNMP commands (v1 and v2). This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

Use the `no` form of this command to remove the specified community string.
Network Management Protocol (SNMP) Commands

Syntax

```plaintext
snmp-server community community-string [ro | rw | su] [ip-address | ipv6-address] [mask mask | prefix prefix-length] [view view-name]

no snmp-server community community-string [ip-address]
```

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters). This string is used as an input parameter to `snmp-server user` for SNMP v3.
- **ro**—Specifies read-only access (default)
- **rw**—Specifies read-write access
- **su**—Specifies SNMP administrator access
- **view view-name**—Specifies the name of a view configured using the command `snmp-server view` (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for `su`, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)
- **ip-address**—Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet’s source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.

Default Configuration

No community is defined

Command Mode

Global Configuration mode
User Guidelines

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The view-name is used to restrict the access rights of a community string. When a view-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also).

Example

Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

14.3 snmp-server community-group

Use `snmp-server community-group` to configure access rights to a user group. The group must exist in order to be able to specify the access rights. This command configures both SNMP v1 and v2.

Syntax

```
snmp-server community-group community-string group-name [ip-address | ipv6-address] [mask mask /prefix prefix-length]
```

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters). This string is used as an input parameter to `snmp-server user` for SNMP v3.

- **ip-address**—Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
• **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet’s source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.

• **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.

• **group-name**—This is the name of a group configured using `snmp-server group` with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)

**Default Configuration**
No community is defined

**Command Mode**
Global Configuration mode

**User Guidelines**
The **group-name** is used to restrict the access rights of a community string. When a group-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

**Example**

Defines a password **tom** for the group **abcd** that enables this group to access the management station 1.1.1.121 with prefix 8.

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

### 14.4  `snmp-server source-interface`

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface`
command in Global Configuration mode. To returned to the default, use the no form of this command.

Syntax

```
snmp-server source-interface {traps | informs} interface-id
no snmp-server source-interface [traps | informs]
```

Parameters

- **traps**—Specifies the SNMP traps interface.
- **informs**—Specifies the SNMP informs.
- **interface-id**—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

If no parameters are specified in no snmp-server source-interface, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to send a SNMP trap or inform.

Use the **no snmp-server source-interface traps** command to remove the source interface for SNMP traps.

Use the **no snmp-server source-interface informs** command to remove the source interface for SNMP informs.

Use the **no snmp-server source-interface** command to remove the source interface for SNMP traps and informs.
Example
The following example configures the VLAN 10 as the source interface for traps.

```plaintext
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```

### 14.5 `snmp-server source-interface-ipv6`

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface-ipv6` command in Global Configuration mode. To returned to the default, use the `no` form of this command.

**Syntax**

```plaintext
snmp-server source-interface-ipv6 {traps | informs} interface-id
no snmp-server source-interface-ipv6 {traps | informs} interface-id
```

**Parameters**

- `traps`—Specifies the SNMP traps interface.
- `informs`—Specifies the SNMP traps informs.
- `interface-id`—Specifies the source interface.

**Default Configuration**

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

If no parameters are specified in `no snmp-server source-interface-ipv6`, the default is both traps and informs.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.
If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to send a SNMP trap or inform.

Use the `no snmp-server source-interface-ipv6 traps` command to remove the source IPv6 interface for SNMP traps.

Use the `no snmp-server source-interface-ipv6 informs` command to remove the source IPv6 interface for SNMP informs.

Use the `no snmp-server source-interface-ipv6` command to remove the source IPv6 interface for SNMP traps and informs.

**Example**

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

### 14.6 snmp-server view

The `snmp-server view` Global Configuration mode command creates or updates an SNMP view. Use the `no` form of this command to remove an SNMP view.

**Syntax**

```
snmp-server view view-name oid-tree {included | excluded}
no snmp-server view view-name [oid-tree]
```

**Parameters**

- **view-name**—Specifies the name for the view that is being created or updated. (Length: 1–30 characters)

- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.

- **included**—Specifies that the view type is included.
• excluded—Specifies that the view type is excluded.

Default Configuration

The following views are created by default:

• Default - Contains all MIBs except for those that configure the SNMP parameters themselves.

• DefaultSuper - Contains all MIBs.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view.

The command’s logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group (this format is specified on the parameters specified in ifEntry).

```
switchxxxxxx(config)# snmp-server view user-view system included
switchxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

14.7 show snmp views

Use the show snmp views Privileged EXEC mode command to display the SNMP views.


**Syntax**

```
show snmp views [viewname]
```

**Parameters**

*viewname*—Specifies the view name. (Length: 1–30 characters)

**Default Configuration**

If *viewname* is not specified, all views are displayed.

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the configured SNMP views.

```
switchxxxxxx# show snmp views

<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>iso</td>
<td>Included</td>
</tr>
<tr>
<td>Default</td>
<td>snmpNotificationMIB</td>
<td>Excluded</td>
</tr>
<tr>
<td>DefaultSuper</td>
<td>iso</td>
<td>Included</td>
</tr>
</tbody>
</table>
```

### 14.8 snmp-server group

Use the **snmp-server group** Global Configuration mode command to configure an SNMP group. Groups are used to map SNMP users to SNMP views (using `snmp-server user`). Use the `no` form of this command to remove an SNMP group.

**Syntax**

```
show snmp views
```

**Parameters**

- `group groupname {v1 | v2 | v3 [noauth | auth | priv] [notify notifyview]] [read readview] [write writeview]}
- `no snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv]}`

**Parameters**

- `group groupname`—Specifies the group name. (Length: 1–30 characters)
- `v1`—Specifies the SNMP Version 1 security model.
• **v2**—Specifies the SNMP Version 2 security model.

• **v3**—Specifies the SNMP Version 3 security model.

• **noauth**—Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.

• **auth**—Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.

• **priv**—Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.

• **notify notifyview**—Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgement. Applicable only to the SNMP version 3 security model. (Length: 1–30 characters)

• **read readview**—Specifies the view name that enables viewing only. (Length: 1–30 characters)

• **write writeview**—Specifies the view name that enables configuring the agent. (Length: 1–30 characters)

**Default Configuration**

No group entry exists.

If **notifyview** is not specified, the notify view is not defined.

If **readview** is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval.

If **writeview** is not specified, the write view is not defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

The group defined in this command is used in `snmp-server user` to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is **(groupname, snmp-version, security-level)**. For snmp-version v1/v2 the security-level is always **noauth**.
Example

The following example attaches a group called `user-group` to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called `user-view` to read-only. User `tom` is then assigned to `user-group`. So that user `tom` has the rights assigned in `user-view`.

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

14.9 show snmp groups

Use the `show snmp groups` Privileged EXEC mode command to display the configured SNMP groups.

Syntax

```
show snmp groups [groupname]
```

Parameters

groupname—Specifies the group name. (Length: 1–30 characters)

Default Configuration

Display all groups.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP groups.

```
switchxxxxxx# show snmp groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Security</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model</td>
<td>Level</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>user-group</td>
<td>V3</td>
<td>priv</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>priv</td>
</tr>
</tbody>
</table>
```
The following table describes significant fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Group name.</td>
</tr>
<tr>
<td>Security</td>
<td>Model: SNMP model in use (v1, v2 or v3).</td>
</tr>
<tr>
<td>Security</td>
<td>Level: Packet authentication with encryption. Applicable to SNMP v3 security only.</td>
</tr>
<tr>
<td>Views</td>
<td>Read: View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.</td>
</tr>
<tr>
<td></td>
<td>Write: View name enabling data entry and managing the agent contents.</td>
</tr>
<tr>
<td></td>
<td>Notify: View name enabling specifying an inform or a trap.</td>
</tr>
</tbody>
</table>

## 14.10 `snmp-server user`

Use the `snmp-server user` Global Configuration mode command to configure a new SNMP Version user. Use the `no` form of the command to remove a user. Use the `encrypted` form of this command to enter the authentication and privacy passwords in encrypted form (see SSD).

**Syntax**

```
snmp-server user username groupname {v1 | v2c | [remote host] v3[auth { md5 | sha} auth-password [priv priv-password]]}
```

```
encrypted snmp-server user username groupname {v1 | v2c | [remote host] v3[auth { md5 | sha} encrypted-auth-password [priv encrypted-priv-password]]}
```

```
no snmp-server user username {v1 | v2c | [remote host] v3[auth { md5 | sha}}
```

**Parameters**

- `username`—Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters).

- `groupname`—The name of the group to which the user belongs. The group should be configured using the command `snmp-server group` with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
Network Management Protocol (SNMP) Commands

- remote host—IP address (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host. See IPv6z Address Conventions.
- v1—Specifies that the user is a v1 user.
- v2c—Specifies that the user is a v2c user.
- v3—Specifies that the user is a v3 user.
- auth—Specifies which authentication level is to be used.
- md5— Specifies the HMAC-MD5-96 authentication level.
- Sha—Specifies the HMAC-SHA-96 authentication level.
- auth-password—Specifies the authentication password. Range: Up to 32 characters.
- encrypted-auth-password—Specifies the authentication password in encrypted format.
- priv-password—Specifies the privacy password (The encryption algorithm used is data encryption standard - DES). Range: Up to 64 characters.
- encrypted-priv-password—Specifies the privacy password in encrypted format.

Default Configuration
No group entry exists.

Command Mode
Global configuration

User Guidelines
For SNMP v1 and v2, this performs the same actions as snmp-server community-group, except that snmp-server community-group configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

When you enter a show running-config command, you do not see a line for this SNMP user. To see if this user has been added to the configuration, type the show snmp user command.

An SNMP EngineID must be defined in order to add SNMPv3 users to the device (in the snmp-server engineID remote commands).
Changing or removing the value of snmpEngineID deletes the SNMPv3 users' database.

The logical key of the command is username.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgement. A configured remote host is also able to manage the device (besides getting the informs).

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the snmp-server engineID remote command. The remote agent’s SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.

**Example**

This example assigns user tom to group abcd using SNMP v1 and v2c. The default is assigned as the engineID. User tom is assigned to group abcd using SNMP v1 and v2c.

```plaintext
switchxxxxxx(config)# snmp-server user tom abcd v1
switchxxxxxx(config)# snmp-server user tom abcd v2c
switchxxxxxx(config)# snmp-server user tom abcd v3
```

### 14.11 show snmp users

Use the **show snmp users** Privileged EXEC mode command to display the configured SNMP users.

**Syntax**

```
show snmp users [username]
```

**Parameters**

- **username**—Specifies the user name. (Length: 1–30 characters)
**Default Configuration**
Display all users.

**Command Mode**
Privileged EXEC mode

**Example**
The following example displays the configured SNMP users

```
switchxxxxxx# show snmp users
User name                        : u1rem
Group name                    : group1
Authentication Algorithm : None
Privacy Algorithm            : None
Remote                           : 11223344556677
Auth Password               :
Priv Password                :

User name                        : qqq
Group name                    : www
Authentication Algorithm : MD5
Privacy Algorithm            : None
Remote                           :
Auth Password               : helloworld1234567890987665
Priv Password                :

User name                            : hello
Group name                        : world
```
Authentication Algorithm : MD5
Privacy Algorithm : DES
Remote :

Auth Password (encrypted):
Z/tC3UF5j0pYfmXm8xeMvclOQ6LQ4GOACCYLRdAgOE6XQKTC
qMLrnpWuHraRIZj

Priv Password (encrypted):
kN1ZHzSl06WWxlkuZVzhLOo1gl5waaNf7Vq6yLBpJdS4N68tL
1tbTRSz2H4c4Q4o

User name : u1noAuth
Group name : group1
Authentication Algorithm : None
Privacy Algorithm : None
Remote :

Auth Password (encrypted):

Priv Password (encrypted):

User name : u1OnlyAuth
Group name : group1
Authentication Algorithm : SHA
Privacy Algorithm : None
Remote :

Auth Password (encrypted):
8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=

Priv Password (encrypted):
14.12 snmp-server filter

The snmp-server filter Global Configuration mode command creates or updates an SNMP server notification filter. Use the no form of this command to remove a notification filter.

Syntax

```
snmp-server filter filter-name oid-tree [included | excluded]
no snmp-server filter filter-name [oid-tree]
```

Parameters

- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the filter in other commands. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.

Default Configuration

No view entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).
Example
The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group (this format depends on the parameters defined in ifEntry).

```
switchxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

14.13 show snmp filters

Use the `show snmp filters` Privileged EXEC mode command to display the defined SNMP filters.

**Syntax**

```
show snmp filters [filtername]
```

**Parameters**

- `filtername`—Specifies the filter name. (Length: 1–30 characters)

**Default Configuration**

If `filtername` is not defined, all filters are displayed.

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the configured SNMP filters.

```
switchxxxxxx# show snmp filters user-filter
<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1</td>
<td>Included</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1.7</td>
<td>Excluded</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.2.2.1.*.1</td>
<td>Included</td>
</tr>
</tbody>
</table>
```
14.14 snmp-server host

Use the **snmp-server host** Global Configuration mode command to configure the host for SNMP notifications: (traps/informs). Use the **no** form of this command to remove the specified host.

**Syntax**

```
snmp-server host {host-ip | hostname} [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host {ip-address | hostname} [traps | informs] [version {1 | 2c | 3}]
```

**Parameters**

- **host-ip**—IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See **IPv6z Address Conventions**.
- **hostname**—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- **trap**—Sends SNMP traps to this host (default).
- **informs**—Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- **1**—SNMPv1 traps are used.
- **2c**—SNMPv2 traps or informs are used.
- **3**—SNMPv2 traps or informs are used.
- **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in **snmp-server user** for v3.
- **Authentication options are available for SNMP v3 only. The following options are available:**
  - **noauth**—Specifies no authentication of a packet.
  - **auth**—Specifies authentication of a packet without encryption.
  - **priv**—Specifies authentication of a packet with encryption.
Network Management Protocol (SNMP) Commands

- **udp-port port**—UDP port of the host to use. The default is 162. (Range: 1–65535)
- **filter filtername**—Filter for this host. If unspecified, nothing is filtered. The filter is defined using `snmp-server filter` (no specific order of commands is imposed on the user). (Range: Up to 30 characters)
- **timeout seconds**—(For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)
- **retries retries**—(For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

**Default Configuration**

Version: SNMP V1
Type of notification: Traps
udp-port: 162
If informs are specified, the default for retries: 3
Timeout: 15

**Command Mode**

Global Configuration mode

**User Guidelines**

The logical key of the command is the list (ip-address/hostname, traps/informs, version).

When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

Use the commands `snmp-server user` and `snmp-server group` to create a user or a group.

**Example**

The following defines a host at the IP address displayed.
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc

### 14.15 snmp-server engineID local

The `snmp-server engineID local` Global Configuration mode command specifies the SNMP engineID on the local device for SNMP v3. Use the `no` form of this command to remove this engine ID.

**Syntax**

```
snmp-server engineID local [engineid-string | default]
no snmp-server engineID local
```

**Parameters**

- **engineid-string**—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)

- **default**—Specifies that the engine ID is created automatically based on the device MAC address.

**Default Configuration**

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

**Command Mode**

Global Configuration mode

**User Guidelines**

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.
As the engineID should be unique within an administrative domain, the following guidelines are recommended:

To configure the engine ID:

- For standalone devices, enter default or configure it explicitly. In the latter case, verify that it is unique within the administrative domain.
- For stackable systems, configure a non-default EngineID, and verify that it is unique within the administrative domain.

Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users database.

The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001

**Example**

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
switchxxxxxx(config)# snmp-server engineid local default
```

The engine-id must be unique within your administrative domain.

Do you wish to continue? [Y/N]Y

The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y

### 14.16 snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the `snmp-server engineID remote` Global Configuration mode command. Use the `no` form of this command to remove the configured engine ID.

**Syntax**

```
snmp-server engineID remote ip-address engineid-string
no snmp-server engineID remote ip-address
```

**Parameters**

- `ip-address` — IPv4, IPv6 or IPv6z address of the remote device. See IPv6z Address Conventions.
- `engineid-string` — The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal...
character strings is two hexadecimal digits. Each byte can be separated by
a period or colon. If the user enters an odd number of hexadecimal digits,
the system automatically prefixes the hexadecimal string with a zero.
(Range: engineid-string5–32 characters. 9–64 hexadecimal digits)

**Default Configuration**

The remote engineID is not configured by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

A remote engine ID is required when an SNMP version 3 inform is configured. The
remote engine ID is used to compute the security digest for authenticating and
encrypting packets sent to a user on the remote host.

### 14.17 show snmp engineID

Use the `show snmp engineID` Privileged EXEC mode command to display the local
SNMP engine ID.

**Syntax**

`show snmp engineID`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the SNMP engine ID.

```
switchxxxxxx # show snmp engineID
```
Local SNMP engineID: 08009009020C0B099C075878
IP address    Remote SNMP engineID
------------  -------------------------------
172.16.1.1    08009009020C0B099C075879

14.18  snmp-server enable traps

Use the **snmp-server enable traps** Global Configuration mode command to enable the device to send all SNMP traps. Use the **no** form of the command to disable all SNMP traps.

**Syntax**

```
snmp-server enable traps
no snmp-server enable traps
```

**Default Configuration**

SNMP traps are enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

If no **snmp-server enable traps** has been entered, you can enable failure traps by using **snmp-server trap authentication** as shown in the example.

**Example**

The following example enables SNMP traps except for SNMP failure traps.

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```

14.19  snmp-server trap authentication

Use the **snmp-server trap authentication** Global Configuration mode command to enable the device to send SNMP traps when authentication fails. Use the **no** form of this command to disable SNMP failed authentication traps.
Syntax
snmp-server trap authentication
no snmp-server trap authentication

Parameters
N/A

Default Configuration
SNMP failed authentication traps are enabled.

Command Mode
Global Configuration mode

User Guidelines
The command snmp-server enable traps enables all traps including failure traps. Therefore, if that command is enabled (it is enabled by default), this command is not necessary.

Example
The following example disables all SNMP traps and enables only failed authentication traps.

switchxxxxxxx(config)# no snmp-server enable traps
switchxxxxxxx(config)# snmp-server trap authentication

14.20 snmp-server contact

Use the snmp-server contact Global Configuration mode command to set the value of the system contact (sysContact) string. Use the no form of the command to remove the system contact information.

Syntax
snmp-server contact text
no snmp-server contact
Parameters

text—Specifies system contact information. (Length: 1–160 characters)

Default Configuration
N/A

Command Mode
Global Configuration mode

Example
The following example sets the system contact information to Technical_Support.

switchxxxxxx(config)# snmp-server contact Technical_Support

14.21  snmp-server location

Use the snmp-server location Global Configuration mode command to set the value of the system location string. Use the no form of this command to remove the location string.

Syntax

snmp-server location text
no snmp-server location

Parameters

text—Specifies the system location information. (Length: 1–160 characters)

Default Configuration
N/A

Command Mode
Global Configuration mode
Example

The following example sets the device location to New_York.

```
switchxxxxxx(config)# snmp-server location New_York
```

14.22 snmp-server set

Use the `snmp-server set` Global Configuration mode command to define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command.

**Syntax**

```
snmp-server set variable-name name value [name2 value2...]
```

**Parameters**

- `variable-name`—Specifies an SNMP MIB variable name, which must be a valid string.
- `name value`—Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**User Guidelines**

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command. To generate configuration files that support those situations, the system uses `snmp-server set`. This command is not intended for the end user.
Example
The following example configures the scalar MIB sysName with the value TechSupp.

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

### 14.23 snmp trap link-status

Use the `snmp trap link-status` Interface Configuration mode command to enable link-status generation of SNMP traps. Use the `no` form of this command to disable generation of link-status SNMP traps.

**Syntax**

```
snmp trap link-status
no snmp trap link-status
```

**Parameters**

N/A

**Default Configuration**

Generation of SNMP link-status traps is enabled

**Command Mode**

Interface Configuration mode

**Example**

The following example disables generation of SNMP link-status traps.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# no snmp trap link-status
```

### 14.24 show snmp

Use the `show snmp` Privileged EXEC mode command to display the SNMP status.
Syntax

show snmp

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:

<table>
<thead>
<tr>
<th>Community-String</th>
<th>Community-Access</th>
<th>View name</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>read only</td>
<td>user-view</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>private</td>
<td>read write</td>
<td>Default</td>
<td>172.16.1.1/10</td>
<td></td>
</tr>
<tr>
<td>private</td>
<td>su</td>
<td>DefaultSuper</td>
<td>172.16.1.1</td>
<td></td>
</tr>
<tr>
<td>Community-string</td>
<td>Group name</td>
<td>IP Address</td>
<td>Mask</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td>public</td>
<td>user-group</td>
<td>All</td>
<td>Router</td>
<td></td>
</tr>
</tbody>
</table>

Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Community</th>
<th>Version</th>
<th>UDP Port</th>
<th>Filter</th>
<th>TO Sec</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.122.173.42</td>
<td>Trap</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>192.122.173.42</td>
<td>Inform</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>

Version 3 notifications
```
The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community-string</td>
<td>The community access string permitting access to SNMP.</td>
</tr>
<tr>
<td>Community-access</td>
<td>The permitted access type—read-only, read-write, super access.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The management station IP Address.</td>
</tr>
<tr>
<td>Target Address</td>
<td>The IP address of the targeted recipient.</td>
</tr>
<tr>
<td>Version</td>
<td>The SNMP version for the sent trap.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Username</th>
<th>Security</th>
<th>UDP Port</th>
<th>Filter Name</th>
<th>TO Sec</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.122.173.42</td>
<td>Inform</td>
<td>Bob</td>
<td>Priv</td>
<td>162</td>
<td>TO Sec</td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>

System Contact: Robert
System Location: Marketing
Web Server Commands

15.1 ip http server

Use the ip http server Global Configuration mode command to enable configuring and monitoring the device from a web browser. Use the no form of this command to disable this function.

Syntax

ip http server
no ip http server

Parameters

N/A

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

Example

The following example enables configuring the device from a web browser.

switchxxxxxx(config)# ip http server

15.2 ip http port

The ip http port Global Configuration mode command specifies the TCP port used by the web browser interface. Use the no form of this command to restore the default configuration.

Syntax

ip http port port-number
no ip http port

Parameters
port port-number—For use by the HTTP server. (Range: 0–65534)

Default Configuration
The default port number is 80.

Command Mode
Global Configuration mode

Example
The following example configures the http port number as 100.

switch_xxxxxxx(config)# ip http port 100

15.3 ip http timeout-policy

Use the ip http timeout-policy Global Configuration mode command to set the interval for the system to wait for user input in http/https sessions before automatic logoff. Use the no form of this command to return to the default value.

Syntax
ip http timeout-policy idle-seconds [http-only | https-only]
no ip http timeout-policy

Parameters
idle-seconds—Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)

http-only —The timeout is specified only for http
https-only— The timeout is specified only for https

Default Configuration
600 seconds
Command Mode
Global Configuration mode

User Guidelines
To specify no timeout, enter the `ip http timeout-policy 0` command.

Example
The following example configures the http timeout to be 1000 seconds.

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

15.4 `ip http secure-server`
Use the `ip http secure-server` Global Configuration mode command to enable the device to be configured or monitored securely from a browser. Use the `no` form of this command to disable this function.

Syntax
`ip http secure-server`
`no ip http secure-server`

Parameters
N/A

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
After this command is used, you must generate a certificate using `crypto certificate generate`. If no certificate is generated, this command has no effect.

Example
15.5 ip https certificate

Use the `ip https certificate` Global Configuration mode command to configure the active certificate for HTTPS. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
ip https certificate number
no ip https certificate
```

**Parameters**

*number*—Specifies the certificate number. (Range: 1–2)

**Default Configuration**

The default certificate number is 1.

**Command Mode**

Global Configuration mode

**User Guidelines**

First, use `crypto certificate generate` to generate one or two HTTPS certificates. Then use this command to specify which is the active certificate.

**Example**

The following example configures the active certificate for HTTPS.

```
switchxxxxxx(config)# ip https certificate 2
```

15.6 show ip http

The `show ip http` EXEC mode command displays the HTTP server configuration.
Syntax
show ip http

Command Mode
EXEC mode

Example
The following example displays the HTTP server configuration.

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes
```

15.7 show ip https
The `show ip https` Privileged EXEC mode command displays the HTTPS server configuration.

Syntax
show ip https

Command Mode
Privileged EXEC mode

Example
The following example displays the HTTPS server configuration.

```
switchxxxxxx# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes)
Certificate 1 is active
Issued by: www.verisign.com
```
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
16.1 ip telnet server

Use the `ip telnet server` Global Configuration mode command to enable the device as a Telnet server that accepts connection requests from remote Telnet clients. Remote Telnet clients can configure the device through the Telnet connections.

Use the `no` form of this command to disable the Telnet server functionality on the device.

**Syntax**

- `ip telnet server`
- `no ip telnet server`

**Default Configuration**

The Telnet server functionality on the device is Disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

The device can be enabled to accept connection requests from both remote SSH and Telnet clients. It is recommended that the remote client connects to the device using SSH (as opposed to Telnet), since SSH is a secure protocol and Telnet is not. To enable the device to be a SSH server, use the `ip ssh server` Global Configuration mode command.

**Example**

The following example enables the device to be configured from a Telnet server.

```
switchxxxxxx(config)# ip telnet server
```
16.2  ip ssh server

The `ip ssh server` Global Configuration mode command enables the device to be an SSH server and so to accept connection requests from remote SSH clients. Remote SSH clients can manage the device through the SSH connection.

Use the `no` form of this command to disable the SSH server functionality from the device.

Syntax

```
ip ssh server
no ip ssh server
```

Default Configuration

The SSH server functionality is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The device as a SSH server generates the encryption keys automatically.

To generate new SSH server keys, use the `crypto key generate dsa` and `crypto key generate rsa` Global Configuration mode commands.

Example

The following example enables configuring the device to be an SSH server.

```
switchxxxxxx(config)# ip ssh server
```

16.3  ip ssh port

The `ip ssh port` Global Configuration mode command specifies the TCP port used by the SSH server. Use the `no` form of this command to restore the default configuration.

Syntax

```
ip ssh port port-number
```

no ip ssh port

Parameters

port-number—Specifies the TCP port number to be used by the SSH server.
(Range: 1–65535)

Default Configuration

The default TCP port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that TCP port number 8080 is used by the SSH server.

switchxxxxxx(config)# ip ssh port 8080

16.4 ip ssh password-auth

Use the `ip ssh password-auth` Global Configuration mode command to enable password authentication of incoming SSH sessions.

Use the `no` form of this command to disable this function.

Syntax

ip ssh password-auth
no ip ssh password-auth

Default Configuration

Password authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode
User Guidelines

This command enables password key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

Example

The following example enables password authentication of the SSH client.

```
switchxxxxxxx(config)# ip ssh password-auth
```

16.5 `ip ssh pubkey-auth`

Use the `ip ssh pubkey-auth` Global Configuration mode command to enable public key authentication of incoming SSH sessions.

Use the `no` form of this command to disable this function.

Syntax

```
ip ssh pubkey-auth [auto-login]
no ip ssh pubkey-auth
```

Parameters

- `auto-login`— Specifies that the device management AAA authentication (CLI login) is not needed. By default, the login is required after the SSH authentication.

Default Configuration

Public Key authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode
**User Guidelines**

This command enables public key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device, except if the auto-login parameter was specified.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

If the `auto-login` keyword is specified for SSH authentication by public key, then management access is granted if SSH authentication succeeds and the name of SSH used is found in the local user database. The device management AAA authentication is transparent to the user. If the user name is not in the local user database, then the user receives a warning message, and the user will need to pass the device management AAA authentication independent to the SSH authentication.

If the `auto-login` keyword is not specified, management access is granted only if the user engages and passes both SSH authentication and device management AAA authentication independently. If no SSH authentication method is enabled, then management access is granted only if the user is AAA authenticated by the device management. No SSH authentication method means SSH is enabled but neither SSH authentication by public key nor password is enabled.

**Example**

The following example enables authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh pubkey-auth
```

**16.6 crypto key pubkey-chain ssh**

The `crypto key pubkey-chain ssh` Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify device public keys, such as SSH client public keys.

**Syntax**

```
crypto key pubkey-chain ssh
```
**Default Configuration**

Keys do not exist.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command when you want to manually specify SSH client’s public keys.

**Example**

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to the user ‘bob’.

```
switchxxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxxx(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADQABAAABAQAQCvTvNwFwI
Al4kpqIw9GBRonZQxjHKcqKL6rM1Q+
ZNXfZSkvHG+QusIZ/761LMFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJkJ67IOU/zfwOllg
kTwm175QR?9hujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWw08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCK0N/W9a/tnkm1shRE7D17l+w3fNIOA
6w9o4t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rm5nhqNdAtN/4oJfe8166DqVX1gWmN
zNR4DYDvSzq01DnwCAC8Qh
```

**16.7 user-key**

The **user-key** SSH Public Key-string Configuration mode command associates a username with a manually-configured SSH public key.
Use the **no user-key** command to remove an SSH user and the associated public key.

**Syntax**

```
user-key username {rsa | dsa}
no user-key username
```

**Parameters**

- **username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- **rsa**—Specifies that the RSA key pair is manually configured.
- **dsa**—Specifies that the DSA key pair is manually configured.

**Default Configuration**

No SSH public keys exist.

**Command Mode**

SSH Public Key-string Configuration mode

**User Guidelines**

After entering this command, the existing key, if any, associated with the user will be deleted. You must follow this command with the **key-string** command to configure the key to the user. **Example**

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl16.8 key-string
```

### **16.8 key-string**

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.
Syntax

key-string \[row\] key-string

Parameters

- row—Specifies the SSH public key row by row. The maximum length of a row is 160 characters.
- key-string—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

Default Configuration

Keys do not exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the key-string SSH Public Key-string Configuration mode command without the row parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the key-string row SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a key-string row command.

The UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client ‘bob’.

switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Telnet, Secure Shell (SSH) and Secure Login (Slogin) Commands

Vu4GRfpSWoQUvV35LqJkJk67IGU/zfwo11g
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd051DX2IE3QWu08licglk02LYciz
+Z4TrEU/9FJxwPiVOj+c+KBXuR0juNg5nFYsY
0Zck0N/W9a/tnkm1shRE7Di71+w3fNiQA
6w9o44t6+AINEICBCCA4ycF6zMaT1weFWwX6f+
Rmt5nhqdAtN/4oJfce166DqVX1gWmN
zNR4DYdsvZg01DnwCAC8Qh
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row AAAAB3Nza
switchxxxxxx(config-pubkey-key)# key-string row C1yc2

16.9 show ip ssh

The show ip ssh Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Command Mode

Privileged EXEC mode
Example

The following example displays the SSH server configuration.

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled with auto-login.
SSH Password Authentication is enabled.
Active incoming sessions:
```

```
IP Address         SSH Username   Version Cipher  Auth Code
------------------ --------------- ------ ------ -----------
172.16.0.1         John Brown     1.5    3DES   HMAC-SHA1
182.20.2.1         Bob Smith      1.5    3DES   Password
```

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The client address</td>
</tr>
<tr>
<td>SSH Username</td>
<td>The user name</td>
</tr>
<tr>
<td>Version</td>
<td>The SSH version number</td>
</tr>
<tr>
<td>Cipher</td>
<td>The encryption type (3DES, Blowfish, RC4)</td>
</tr>
<tr>
<td>Auth Code</td>
<td>The authentication Code (HMAC-MD5, HMAC-SHA1) or Password</td>
</tr>
</tbody>
</table>

16.10 show crypto key pubkey-chain ssh

The `show crypto key pubkey-chain ssh` Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

```
show crypto key pubkey-chain ssh [username username] [fingerprint
[bubble-babble / hex]
```
Parameters

- **username username**—Specifies the remote SSH client username. (Length: 1–48 characters)

- **fingerprint {bubble-babble | hex}**—Specifies the fingerprint display format. The possible values are:
  - **bubble-babble**—Specifies that the fingerprint is displayed in Bubble Babble format.
  - **hex**—Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username  Fingerprint
----------- ----------------------------------------------------------

switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username  Fingerprint
----------- ----------------------------------------------------------
```
17.1 line

The line Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

```
line {console | telnet | ssh}
```

Parameters

- **console**—Enters the terminal line mode.
- **telnet**—Configures the device as a virtual terminal for remote access (Telnet).
- **ssh**—Configures the device as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) access.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)#
```

17.2 speed

Use the speed command in Line Configuration mode to set the line baud rate.

Use the no form of this command to restore the default configuration.
Syntax
speed \textit{bps}
no speed

Parameters
\textbf{bps}—Specify the baud rate in bits per second (bps). Possible values are 4800, 9600, 19200, 38400, 57600, and 115200.

Default Configuration
The default speed is 115200 bps.

Command Mode
Line Configuration mode

User Guidelines
The configured speed is only applied when \texttt{autobaud} is disabled. This configuration applies to the current session only.

Example
The following example configures the line baud rate as 9600 bits per second.

```
switchxxxxxx(config-line)# speed 9600
```

17.3 \texttt{autobaud}

Use the \texttt{autobaud} command in Line Configuration mode to configure the line for automatic baud rate detection (autobaud).

Use the \texttt{no} form of this command to disable automatic baud rate detection.

Syntax
autobaud
no autobaud

Default Configuration
Automatic baud rate detection is enabled.
Command Mode
Line Configuration mode

User Guidelines
When this command is enabled, it is activated as follows: connect the console to the device and press the Enter key twice. The device detects the baud rate automatically.

Example
The following example enables autobaud.

```plaintext
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# autobaud
```

17.4 exec-timeout
The `exec-timeout` Line Configuration mode command sets the session idle time interval, during which the system waits for user input before automatic logoff. Use the `no` form of this command to restore the default configuration.

Syntax
`exec-timeout minutes [seconds]`
`no exec-timeout`

Parameters
- `minutes`—Specifies the number of minutes. (Range: 0-65535)
- `seconds`—Specifies the number of seconds. (Range: 0-59)

Default Configuration
The default idle time interval is 10 minutes.

Command Mode
Line Configuration mode
**Example**

The following example sets the telnet session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-timeout 20 10
```

**17.5 show line**

The *show line* EXEC mode command displays line parameters.

**Syntax**

```
show line [console / telnet / ssh]
```

**Parameters**

- **console**—Displays the console configuration.
- **telnet**—Displays the Telnet configuration.
- **ssh**—Displays the SSH configuration.

**Default Configuration**

If the line is not specified, all line configuration parameters are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the line configuration.

```
switchxxxxxx# show line
Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
```
Databits: 8
Parity: none
Stopbits: 1
Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
SSH configuration:
SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
18.1 bonjour enable

Use the **bonjour enable** Global Configuration mode command to enable Bonjour globally. Use the **no** format of the command to disable Bonjour globally.

**Syntax**

- `bonjour enable`
- `no bonjour enable`

**Default Configuration**

Enable

**Command Mode**

Global Configuration mode

**Examples**

```
switchxxxxxx(conf)# bonjour enable
```

18.2 bonjour interface range

Use the **bonjour interface range** Global Configuration mode command to add L2 interfaces to the Bonjour L2 interface list. Use the **no** format of the command to remove L2 interfaces from this list.

**Syntax**

- `bonjour interface range {interface-list}`

**Parameters**

- **interface-list**—Specifies a list of interfaces, which can be of the following types:
  - Ethernet port
  - Port-channel
### VLAN

**Default Configuration**
The list is empty.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command can only be used if the device is in Layer 3 (router) mode.

**Examples**

```plaintext
switchxxxxxx(config)# bonjour interface range gi1/1/1-3
```

### 18.3 show bonjour

Use the `show bonjour` Privileged EXEC mode command to display Bonjour information.

**Syntax**

```
show bonjour [interface-id]
```

**Parameters**

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types:

- Ethernet port
- Port-channel
- VLAN

**Command Mode**

Privileged EXEC mode

**Examples**

Layer 2:
Bonjour Commands

```
switchxxxxx# show bonjour
Bonjour status: enabled
L2 interface status: Up
IP Address: 10.5.226.46
Service     Admin Status     Oper Status
-------     ------------     --------------
csco-sb     enabled              enabled
http        enabled              enabled
https       enabled              disabled
ssh         enabled              disabled
telnet      enabled              disabled

Layer 3:

switchxxxxx# show bonjour
Bonjour global status: enabled
Bonjour L2 interfaces list: vlans 1
Service     Admin Status     Oper Status
-------     ------------     --------------
csco-sb     enabled              enabled
http        enabled              enabled
https       enabled              disabled
ssh         enabled              disabled
telnet      enabled              disabled
```
19.1 aaa authentication login

Use the **aaa authentication login** Global Configuration mode command to set one or more authentication methods to be applied during login. A list of authentication methods may be assigned a list name, and this list name can be used in **login authentication aaa authentication enable**. Use the **no** form of this command to restore the default authentication method.

**Syntax**

```
aaa authentication login {default | list-name} method1 [method2...]
aaa authentication login list-name method1 method2...
no aaa authentication login {default | list-name}
```

**Parameters**

- **default**—Uses the authentication methods that follow this argument as the default method list when a user logs in (this list is unnamed).
- **list-name**—Specifies a name of a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- **method1 [method2...]**—Specifies a list of methods that the authentication algorithm tries (in the given sequence). Each additional authentication method is used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Select one or more methods from the following list:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the locally-defined usernames for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>
Default Configuration

If no methods are specified, the default are the locally-defined users and passwords. This is the same as entering the command `aaa authentication login local`.

**NOTE** If no authentication method is defined, console users can log in without any authentication verification.

Command Mode

Global Configuration mode

User Guidelines

Create a list of authentication methods by entering this command with the `list-name` parameter where `list-name` is any character string. The method arguments identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created with this command are used with `login authentication aaa authentication enable`.

`no aaa authentication login list-name` deletes a list-name only if it has not been referenced by another command.

Example

The following example sets the authentication login methods for the console.

```
switchxxxxxx (config)# aaa authentication login authen-list radius local none
switchxxxxxx (config)#line console
switchxxxxxx (config-line)#login authentication authen-list
```

### 19.2 aaa authentication enable

The `aaa authentication enable` Global Configuration mode command sets one or more authentication methods for accessing higher privilege levels. A user, who
logons with a lower privilege level, must pass these authentication methods to access a higher level.

To restore the default authentication method, use the no form of this command.

**Syntax**

`aaa authentication enable {default | list-name} method [method2...]`

`no aaa authentication enable {default | list-name}`

**Parameters**

- `default`—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.

- `list-name` —Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)

- `method [method2...]`—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify none as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Configuration**

The `enable password` command defines the default authentication login method. This is the same as entering the command `aaa authentication enable default enable`.

On a console, the enable password is used if a password exists. If no password is set, authentication still succeeds. This is the same as entering the command `aaa authentication enable default enable none`. 
Command Mode
Global Configuration mode

User Guidelines
Create a list by entering the `aaa authentication enable list-name method1 [method2...]` command where `list-name` is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created by this command are used with `enable authentication`.

All `aaa authentication enable` requests sent by the device to a RADIUS server include the username `$enabx$`, where `x` is the requested privilege level.

All `aaa authentication enable` requests sent by the device to a TACACS+ server include the username that is entered for login authentication.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify `none` as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

`no aaa authentication enable list-name` deletes list-name if it has not been referenced.

Example
The following example sets the enable password for authentication for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

19.3 login authentication

The `login authentication` Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the `no` form of this command to restore the default authentication method.

Syntax

```
login authentication {default | list-name}
```

no login authentication

Parameters

- **default**—Uses the default list created with the `aaa authentication login` command.
- **list-name**—Uses the specified list created with `aaa authentication login`.

Default Configuration

The default is the `aaa authentication login` command default.

Command Mode

Line Configuration mode

Examples

**Example 1** - The following example specifies the login authentication method as the default method for a console session.

```bash
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication default
```

**Example 2** - The following example sets the authentication login methods for the console as a list of methods.

```bash
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

### 19.4 enable authentication

The `enable authentication` Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the `no` form of this command to restore the default authentication method.
Syntax

enable authentication {default | list-name}

no enable authentication

Parameters

- **default**—Uses the default list created with the `aaa authentication enable` command.

- **list-name**—Uses the specified list created with the `aaa authentication enable` command.

Default Configuration

The default is the `aaa authentication enable` command default.

Command Mode

Line Configuration mode

Example

**Example 1** - The following example specifies the authentication method as the default method when accessing a higher privilege level from a console.

```bash
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

**Example 2** - The following example sets a list of authentication methods for accessing higher privilege levels.

```bash
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

### 19.5 ip http authentication

The `ip http authentication` Global Configuration mode command specifies authentication methods for HTTP server access. Use the `no` form of this command to restore the default authentication method.
Syntax

```
ip http authentication aaa login-authentication method1 [method2...]
no ip http authentication aaa login-authentication
```

Parameters

```
method [method2...]—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify none as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

Default Configuration

The local user database is the default authentication login method. This is the same as entering the `ip http authentication local` command.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for HTTP and HTTPS server users.

Example

The following example specifies the HTTP access authentication methods.

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius local none
```
19.6 show authentication methods

The show authentication methods Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the authentication configuration.

```
switchxxxxxx# show authentication methods
Login Authentication Method Lists
-------------------------------
Default: Radius, Local, Line
Console_Login: Line, None
Enable Authentication Method Lists
-------------------------------
Default: Radius, Enable
Console_Enable: Enable, None

Line         Login Method List    Enable Method List
------------- -----------            -------------
Console      Console_Login        Console_Enable
Telnet       Default              Default
SSH          Default              Default
HTTP: Radius, local
HTTPS: Radius, local
Dot1x: Radius
```
19.7 **password**

Use the `password` Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the `no` form of this command to return to the default password.

**Syntax**

```
password password [encrypted]
no password
```

**Parameters**

- `password`—Specifies the password for this line. (Length: 0–159 characters)
- `encrypted`—Specifies that the password is encrypted and copied from another device configuration.

**Default Configuration**

No password is defined.

**Command Mode**

Line Configuration mode

**Example**

The following example specifies the password ‘secret’ on a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secret
```

19.8 **enable password**

Use the `enable password` Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the `no` form of this command to return to the default password.

When the administrator configures a new `enable` password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword `encrypted` and the encrypted value.
If the administrator wants to manually copy a password that was configured on one switch (for instance, switch B) to another switch (for instance, switch A), the administrator must add `encrypted` in front of this encrypted password when entering the `enable` command in switch A. In this way, the two switches will have the same password.

**Syntax**

`enable password [level privilege-level] [unencrypted-password | encrypted encrypted-password]`

`no enable password [level level]`

**Parameters**

- `level privilege-level`—Level for which the password applies. If not specified, the level is 15. (Range: 1–15)
- `password unencrypted-password`—Password for this level. (Range: 0–159 chars)
- `password encrypted encrypted-password`—Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)

**Default Configuration**

Default for `level` is 15.

Passwords are encrypted by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Passwords are encrypted by default. You only are required to use the `encrypted` keyword when you are actually entering an encrypted keyword.

**Examples**

**Example 1** - The command sets a password that has already been encrypted. It will copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.
Authentication, Authorization and Accounting (AAA) Commands

19.9 service password-recovery

Use the `service password-recovery` Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the `no service password-recovery` command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: “All the configuration and user files were removed”.

Syntax

```
service password-recovery
no service password-recovery
```

Parameters

N/A

Default Configuration

The service password recovery is enabled by default.

Command Mode

Global Configuration mode

User Guidelines
- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.

- If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.

- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

**Example**

The following command disables password recovery:

```
switchxxxxxx(config)# no service password recovery
```

Note that choosing to use Password recovery option in the Boot Menu during the boot process will remove the configuration files and the user files. Would you like to continue? Y/N.

### 19.10 username

Use the `username` Global Configuration mode command to establish a username-based authentication system. Use the `no` form to remove a user name.

**Syntax**

```
username name {nopassword | password password | privilege privilege-level | unencrypted-password | encrypted encrypted-password}
```

```
username name
```

```
no username name
```

**Parameters**

- `name`—The name of the user. (Range: 1–20 characters)
- **nopassword**—No password is required for this user to log in.
- **password**—Specifies the password for this username. (Range: 1–64)
- **unencrypted-password**—The authentication password for the user. (Range: 1–159)
- **encrypted encrypted-password**—Specifies that the password is MD5 encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)
- **privilege privilege-level**—Privilege level for which the password applies. If not specified the level is 15. (Range: 1–15).

**Default Configuration**

No user is defined.

**Command Mode**

Global Configuration mode

**Usage Guidelines**

See **User (Privilege) Levels** for an explanation of privilege levels.

- The last level 15 user (regardless of whether it is the default user or any user) cannot be removed.
- The last level 15 user (regardless of whether it is the default user or any user) cannot be demoted

**Examples**

**Example 1** - Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom privilege 15 password 1234
```

**Example 2** - Sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebe4
```
19.11  show users accounts

The `show users accounts` Privileged EXEC mode command displays information about the users local database.

Syntax

`show users accounts`

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays information about the users local database.

```
switchxxxxxx# show users accounts
```

<table>
<thead>
<tr>
<th>Username</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>15</td>
</tr>
<tr>
<td>Robert</td>
<td>15</td>
</tr>
<tr>
<td>Smith</td>
<td>15</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user name.</td>
</tr>
<tr>
<td>Privilege</td>
<td>The user’s privilege level.</td>
</tr>
</tbody>
</table>
19.12 aaa accounting login

Use the `aaa accounting login` command in Global Configuration mode to enable accounting of device management sessions. Use the `no` form of this command to disable accounting.

**Syntax**

```plaintext
aaa accounting login start-stop group {radius | tacacs+}
no aaa accounting login start-stop
```

**Parameters**

- **group radius**— Uses a RADIUS server for accounting.
- **group tacacs+**— Uses a TACACS+ server for accounting.

**Default Configuration**

Disabled

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a “start”/“stop” messages to a RADIUS server when a user logs in / logs out respectively.

The device uses the configured priorities of the available RADIUS/TACACS+ servers in order to select the RADIUS/TACACS+ server.

The following table describes the supported RADIUS accounting attributes values, and in which messages they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Start Message</th>
<th>Stop Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>Yes</td>
<td>Yes</td>
<td>User’s identity.</td>
</tr>
</tbody>
</table>
The following table describes the supported TACACS+ accounting arguments and in which messages they are sent by the switch:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Start Message</th>
<th>Stop Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_id</td>
<td>A unique accounting session identifier.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>user</td>
<td>username that is entered for login authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>rem-addr</td>
<td>IP address of the user</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>elapsed-time</td>
<td>Indicates how long the user was logged in.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>reason</td>
<td>Reports why the session was terminated.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Example

```
switchxxxxxx(config)# aaa accounting login start-stop group tacacs
```
19.13 aaa accounting dot1x

To enable accounting of 802.1x sessions, use the `aaa accounting dot1x` Global Configuration mode command. Use the `no` form of this command to disable accounting.

**Syntax**

```
aaa accounting dot1x start-stop group radius
no aaa accounting dot1x start-stop group radius
```

**Parameters**

N/A

**Default Configuration**

Disabled

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends a “start”/“stop” messages to a RADIUS server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available RADIUS servers in order to select the RADIUS server.

If a new supplicant replaces an old supplicant (even if the port state remains authorized), the software sends a “stop” message for the old supplicant and a “start” message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends “start”/“stop” messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends “start”/“stop” messages only for the supplicant that has been authenticated.

The software does not send “start”/“stop” messages if the port is force-authorized.

The software does not send “start”/“stop” messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.
The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Start</th>
<th>Stop</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name (1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Supplicant's identity.</td>
</tr>
<tr>
<td>NAS-IP-Address (4)</td>
<td>Yes</td>
<td>Yes</td>
<td>The switch IP address that is used for the session with the RADIUS server.</td>
</tr>
<tr>
<td>NAS-Port (5)</td>
<td>Yes</td>
<td>Yes</td>
<td>The switch port from where the supplicant has logged in.</td>
</tr>
<tr>
<td>Class (25)</td>
<td>Yes</td>
<td>Yes</td>
<td>Arbitrary value is included in all accounting packets for a specific session.</td>
</tr>
<tr>
<td>Called-Station-ID (30)</td>
<td>Yes</td>
<td>Yes</td>
<td>The switch MAC address.</td>
</tr>
<tr>
<td>Calling-Station-ID (31)</td>
<td>Yes</td>
<td>Yes</td>
<td>The supplicant MAC address.</td>
</tr>
<tr>
<td>Acct-Session-ID (44)</td>
<td>Yes</td>
<td>Yes</td>
<td>A unique accounting identifier.</td>
</tr>
<tr>
<td>Acct-Authentic (45)</td>
<td>Yes</td>
<td>Yes</td>
<td>Indicates how the supplicant was authenticated.</td>
</tr>
<tr>
<td>Acct-Session-Time (46)</td>
<td>No</td>
<td>Yes</td>
<td>Indicated how long the supplicant was logged in.</td>
</tr>
<tr>
<td>Acct-Terminate-Cause (49)</td>
<td>No</td>
<td>Yes</td>
<td>Reports why the session was terminated.</td>
</tr>
<tr>
<td>Nas-Port-Type (61)</td>
<td>Yes</td>
<td>Yes</td>
<td>Indicates the supplicant physical port type.</td>
</tr>
</tbody>
</table>

Example

switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
19.14 show accounting

The show accounting EXEC mode command displays information as to which type of accounting is enabled on the switch.

Syntax

show accounting

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays information about the accounting status.

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

19.15 passwords complexity enable

Use the passwords complexity enable Global Configuration mode command to enforce minimum password complexity. The no form of this command disables enforcing password complexity.

Syntax

passwords complexity enable

no passwords complexity enable

Parameters

N/A
Default Configuration
Enabled

Command Mode
Global Configuration mode

User Guidelines
If password complexity is enabled by default, the user is forced to enter a password that:

- Has a minimum length of 8 characters.
- Contains characters from at least 3 character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Are different from the current password.
- Contains no character that is repeated more than 3 times consecutively.
- Does not repeat or reverse the user name or any variant reached by changing the case of the characters.
- Does not repeat or reverse the manufacturer’s name or any variant reached by changing the case of the characters.

You can control the above attributes of password complexity with specific commands described in this section.

If you have previously configured other complexity settings, then those settings are used. This command does not wipe out the other settings. It works only as a toggle.

Example
The following example configures requiring complex passwords that fulfill the minimum requirements specified in the User Guidelines above.

```
switchxxxxxx(config)# passwords complexity enable
switchxxxxxx#show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
```
Minimal classes: 3

New password must be different than the current: Enabled

Maximum consecutive same characters: 3

New password must be different than the user name: Enabled

New password must be different than the manufacturer name: Enabled

switchcc293e#

19.16 passwords complexity <attributes>

Use the passwords complexity <attributes> Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the no form of these commands to return to default.

Syntax

passwords complexity min-length number

no passwords complexity min-length

passwords complexity min-classes number

no passwords complexity min-classes

passwords complexity not-current

no passwords complexity not-current

passwords complexity no-repeat number

no password complexity no-repeat

passwords complexity not-username

no passwords complexity not-username

passwords complexity not-manufacturer-name

no passwords complexity not-manufacturer-name

Parameters

- min-length number—Sets the minimal length of the password. (Range: 0–64)
- **min-classes number**—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0–4)

- **not-current**—Specifies that the new password cannot be the same as the current password.

- **no-repeat number**—Specifies the maximum number of characters in the new password that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0–16)

- **not-username**—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.

- **not-manufacturer-name**—Specifies that the password cannot repeat or reverse the manufacturer’s name or any variant reached by changing the case of the characters.

**Default Configuration**

The minimal length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All the other controls are enabled by default.

**Command Mode**

Global Configuration mode

**Example**

The following example configures the minimal required password length to 8 characters.

```
switchxxxxxx (config)# passwords complexity min-length 8
```

**19.17 passwords aging**

Use the `passwords aging` Global Configuration mode command to enforce password aging. Use the `no` form of this command to return to default.
Syntax

```
passwords aging days
no passwords aging
```

Parameters

- **days**—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365)

Default Configuration

Enabled and the number of days is 180.

Command Mode

Global Configuration mode

User Guidelines

Aging is relevant only to users of the local database with privilege level 15 and to “enable” a password of privilege level 15.

To disable password aging, use `passwords aging 0`. Using `no passwords aging` sets the aging time to the default.

Example

The following example configures the aging time to be 24 days.

```
switchxxxxxx (config)# passwords aging 24
```

### 19.18 show passwords configuration

The `show passwords configuration` Privileged EXEC mode command displays information about the password management configuration.

Syntax

```
show passwords configuration
```

Parameters

- **N/A**
Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example

switchxxxxxx#show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
New password must be different than the manufacturer name: Enabled
switchcc293e#

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal length</td>
<td>The minimal length required for passwords in the local database.</td>
</tr>
<tr>
<td>Minimal character classes</td>
<td>The minimal number of different types of characters (special characters, integers and so on) required to be part of the password.</td>
</tr>
<tr>
<td>Maximum number of repeated characters</td>
<td>The maximum number of times a single character can be repeated in the password.</td>
</tr>
<tr>
<td>Level</td>
<td>The applied password privilege level.</td>
</tr>
<tr>
<td>Aging</td>
<td>The password aging time in days.</td>
</tr>
</tbody>
</table>
20.1 radius-server host

Use the `radius-server host` Global Configuration mode command to configure a RADIUS server host. Use the `no` form of the command to delete the specified RADIUS server host.

Note: Enter the word `encrypted` before the command to enter a key in its encrypted form.

Syntax

```
radius-server host {ip-address | hostname} [auth-port auth-port-number] [acct-port acct-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [priority priority] [usage {login | dot1.x | all}]
```

```
no radius-server host {ip-address | hostname}
```

Parameters

- `ip-address`—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions
- `hostname`—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- `auth-port auth-port-number`—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- `acct-port-number`—Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
- `timeout timeout`—Specifies the timeout value in seconds. (Range: 1–30)
- `retransmit retries`—Specifies the number of retry retransmissions (Range: 1–15)
- `deadtime deadtime`—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
RADIUS Commands

- **key** *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters). If this parameter is omitted, the globally-configured radius key will be used.

- **key encrypted-*key-string*—Same as key-string, but the key is in encrypted format.

- **priority** *priority*—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)

- **usage** {login | dot1x | all}—Specifies the RADIUS server usage type. The possible values are:
  - **login**—Specifies that the RADIUS server is used for user login parameters authentication.
  - **dot1x**—Specifies that the RADIUS server is used for 802.1x port authentication.
  - **all**—Specifies that the RADIUS server is used for user login authentication and 802.1x port authentication.

- **encrypted-*key-string*—Same as the key-string parameter, but the key is in encrypted form.

**Default Configuration**

The default authentication port number is 1812.

If **retransmit** is not specified, the global value (set in radius-server retransmit) is used.

If **key-string** is not specified, the global value (set in radius-server key) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command or in radius-server host source-interface, the default timeout for radius-server host source-interface is used.

The default usage type is **all**.

**Command Mode**

Global Configuration mode
User Guidelines

To specify multiple hosts, this command is used for each host.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
switchxxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

20.2 radius-server key

Use the `radius-server key` Global Configuration mode command to set the authentication and encryption key for RADIUS communications between the device and the RADIUS daemon.

Use the `no` form of this command to restore the default configuration.

Syntax

```
radius-server key [key-string]
encrypted radius-server key [encrypted-key-string]
```

Parameters

- `key-string`—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

- `encrypted-key-string`—Same as the `key-string` parameter, but the key is in encrypted form.

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode
Example
The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

### 20.3 radius-server retransmit

Use the `radius-server retransmit` Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
radius-server retransmit retries
no radius-server retransmit
```

**Parameters**

`retransmit retries`—Specifies the number of retry retransmissions (Range: 1–15)

**Default Configuration**

The software searches the list of RADIUS server hosts 3 times.

**Command Mode**

Global Configuration mode

**Example**

The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
switchxxxxxx(config)# radius-server retransmit 5
```

### 20.4 radius-server host source-interface

Use the `radius-server host source-interface` Global Configuration mode command to specify the source interface which IPv4 address will be used as the Source
IPv4 address for communication with IPv4 RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

radius-server host source-interface interface-id
no radius-server host source-interface

Parameters

interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 RADIUS servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface vlan 100
```

20.5  radius-server host source-interface-ipv6

Use the radius-server host source-interface-ipv6 Global Configuration mode command to specify the source interface which IPv6 address will be used as the Source IPv6 address for communication with IPv6 RADIUS servers. Use the no form of this command to restore the default configuration.
Syntax
radius-server host source-interface-ipv6 interface-id
no radius-server host source-interface-ipv6

Parameters
interface-id—Specifies the source interface.

Default Configuration
The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode
Global Configuration mode

User Guidelines
If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 RADIUS servers.

Example
The following example configures the VLAN 10 as the source interface.

switchxxxxxx(config)# radius-server host source-interface-ipv6 vlan 100

20.6 radius-server timeout

Use the radius-server timeout Global Configuration mode command to set how long the device waits for a server host to reply. Use the no form of this command to restore the default configuration.

Syntax
radius-server timeout timeout-seconds
no radius-server timeout

Parameters

timeout timeout-seconds—Specifications the timeout value in seconds. (Range: 1–30)

Default Configuration

The default timeout value is 3 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
switchxxxxxx(config)# radius-server timeout 5
```

20.7 radius-server deadtime

Use the radius-server deadtime Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the no form of this command to restore the default configuration.

Syntax

```
radius-server deadtime deadtime
no radius-server deadtime
```

Parameters

deadtime—Specifications the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

Default Configuration

The default deadtime interval is 0.
Command Mode
Global Configuration mode

Example
The following example sets all RADIUS server deadtimes to 10 minutes.

```
switchxxxxxx(config)# radius-server deadtime 10
```

20.8 show radius-servers
Use the show radius-servers Privileged EXEC mode command to display the RADIUS server settings.

Syntax
```
show radius-servers
```

Command Mode
Privileged EXEC mode

Example
The following example displays RADIUS server settings:

```
switchxxxxxx# show radius-servers
  IP address  Port Time                Dead  Auth Out   Retransmission time  Priority Usage
----------  ---- ----  ------------- ------ -------- -------- ------- ------  ------- -----
  172.16.1.1 1812 1813  Global              Global  1        All
  172.16.1.2 1812 1813            Global  8        Global  2        All
```

Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
20.9 show radius-servers key

Use the **show radius-servers key** Privileged EXEC mode command to display the RADIUS server key settings.

**Syntax**

```
show radius-servers key
```

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays RADIUS server key settings:

```
switchxxxxxx# show radius-servers key
IP address       Key (Encrypted)
-----------------  ----
172.16.1.1        Sharon123
172.16.1.2        Bruce123

Global key (Encrypted)
-----------------------
Alice456
```
TACACS+ Commands

21.1 tacacs-server host

Use the tacacs-server host Global Configuration mode command to specify a TACACS+ host. Use the no form of this command to delete the specified TACACS+ host.

Note: Enter the word encrypted before the command to enter a key in its encrypted form.

Syntax

tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [priority priority]

no tacacs-server host {ip-address | hostname}

Parameters

- **host ip-address**—Specifies the TACACS+ server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- **host hostname**—Specifies the TACACS+ server host name. (Length: 1-158 characters. Maximum label length of each part of the host name: 63 characters)
- **single-connection**—Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- **port port-number**—Specifies the TACACS server TCP port number. If the port number is 0, the host is not used for authentication. (Range: 0-65535)
- **timeout timeout**—Specifies the timeout value in seconds. (Range: 1-30)
- **key key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter “”. (Length: 0-128 characters). If this parameter is omitted, the globally-defined key (set in tacacs-server key) will be used.
- **key encrypted-key-string**—Same as key-string, but the key is in encrypted format.
• **priority priority**—Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

**Default Configuration**

No TACACS+ host is specified.

The default port-number is 1812.

If timeout is not specified, the global value (set in tacacs-server timeout) is used.

If key-string is not specified, the global value (set in tacacs-server key) is used.

If the source value is not specified, the global value (set in tacacs-server host source-interface or tacacs-server host source-interface-ipv6) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command or in tacacs-server timeout, the default timeout for tacacs-server timeout is used.

**Command Mode**

Global Configuration mode

**User Guidelines**

Multiple tacacs-server host commands can be used to specify multiple hosts.

**Example**

The following example specifies a TACACS+ host.

```
switchxxxxxx(config)# tacacs-server host 172.16.1.1
```

### 21.2 **tacacs-server key**

Use the **tacacs-server key** Global Configuration mode command to set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the no form of this command to disable the key.

**Syntax**

```
tacacs-server key key-string
```
encrypted tacacs-server key encrypted-key-string

no tacacs-server key

Parameters

- key-string—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)
- encrypted-key-string—Same as key-string, but the key is in encrypted format.

Default Configuration

The default key is an empty string.

Command Mode

Global Configuration mode

Example

The following example sets Enterprise as the authentication encryption key for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server key enterprise
```

### 21.3 tacacs-server timeout

Use the `tacacs-server timeout` Global Configuration mode command to set the interval during which the device waits for a TACACS+ server to reply. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
tacacs-server timeout timeout
no tacacs-server timeout
```

**Parameters**

- timeout—Specifies the timeout value in seconds. (Range: 1-30)
Default Configuration

The default timeout value is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout value to 30 for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server timeout 30
```

### 21.4 tacacs-server host source-interface

Use the `tacacs-server host source-interface` Global Configuration mode command to specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 TACACS+ servers. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
tacacs-server host source-interface interface-id
```

```
no tacacs-server host source-interface
```

**Parameters**

- `interface-id`—Specifies the source interface.

**Default Configuration**

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.
If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 TACAS+ servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface vlan 10
```

### 21.5 tacacs-server host source-interface-ipv6

Use the `tacacs-server host source-interface-ipv6` Global Configuration mode command to specify the source interface which IPv6 address will be used as the Source IPv6 address for communication with IPv6 RADIUS servers. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
tacacs-server host source-interface-ipv6 interface-id
no tacacs-server host source-interface-ipv6
```

**Parameters**

- `interface-id`—Specifies the source interface.

**Default Configuration**

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

**Command Mode**

Global Configuration mode

**User Guidelines**

- If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

- If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.
If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 TACACS+ servers.

Example
The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface-ipv6 vlan 100
```

### 21.6 show tacacs

Use the `show tacacs` Privileged EXEC mode command to display configuration and statistical information for a TACACS+ server.

**Syntax**

```
show tacacs [ip-address]
```

**Parameters**

- `ip-address`—Specifies the TACACS+ server name, IP or IPv6 address.

**Default Configuration**

If `ip-address` is not specified, information for all TACACS+ servers is displayed.

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays configuration and statistical information for all TACACS+ servers

```
switchxxxxxx# show tacacs

IP address Status Port Single Time Priority

Connection Out

-------- ------ -------- ------ --------
172.16.1.1 Connected 49 No Global 1

Global values

---------
Time Out: 3
```
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10

## 21.7 show tacacs key

Use the `show tacacs key` Privileged EXEC mode command to display the configured key of the TACACS+ server.

**Syntax**

```
show tacacs key [ip-address]
```

**Parameters**

- `ip-address`—Specifies the TACACS+ server name or IP address.

**Default Configuration**

If `ip-address` is not specified, information for all TACACS+ servers is displayed.

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays configuration and statistical information for all TACACS+ servers.

```
switchxxxxxx# show tacacs key
IP address    Key (Encrypted)

Global key
(Encrypted)
```

--------------
SYSLOG Commands

22.1 logging on

Use the logging on Global Configuration mode command to control error message logging. This command sends debug or error messages asynchronously to designated locations. Use the no form of this command to disable the logging.

Syntax

logging on
no logging on

Parameters

N/A

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or SYSLOG server. Logging on and off at these destinations can be individually configured using the logging buffered, logging file, and logging on Global Configuration mode commands. However, if the logging on command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example enables logging error messages.

switchxxxxxx(config)# logging on
22.2 logging host

Use the logging host Global Configuration command to log messages to the specified SYSLOG server. Use the no form of this command to delete the SYSLOG server with the specified address from the list of SYSLOG servers.

Syntax

logging host {ip-address | ipv6-address | hostname} [port port] [severity level] [facility facility] [description text]

no logging host {ipv4-address | ipv6-address | hostname}

Parameters

- ip-address—IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or Ipv6z address. See IPv6z Address Conventions.
- hostname—Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- port port—Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- severity level—Limits the logging of messages to the SYSLOG servers to a specified level: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging.
- facility facility—The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- description text—Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

If unspecified, the severity level defaults to Informational.

Command Mode

Global Configuration mode
### User Guidelines

You can use multiple SYSLOG servers.

### Examples

```
switchxxxxxx(config)# logging host 1.1.1.121
```

```
switchxxxxxx(config)# logging host 3000::100/SYSLOG1
```

### 22.3 logging source-interface

Use the `logging source-interface` Global Configuration mode command to specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SYSLOG servers. Use the `no` form of this command to restore the default configuration.

#### Syntax

```
logging source-interface interface-id

no logging source-interface
```

#### Parameters

- `interface-id`—Specifies the source interface.

#### Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

#### Command Mode

Global Configuration mode

#### User Guidelines

- If the source interface is the outgoing interface, the interface IP address belonging to then next hop IPv4 subnet is applied.
- If the source interface is not the outgoing interface, the lowest IPv4 address defined on the source interface is applied.
- If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SYSLOG server.
Example
The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface vlan 100
```

### 22.4 logging source-interface-ipv6

Use the `logging source-interface-ipv6` Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 SYSLOG servers. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
logging source-interface-ipv6 interface-id
no logging source-interface-ipv6
```

**Parameters**

- `interface-id`— Specifies the source interface.

**Default Configuration**

The IPv6 source address is the defined IPv6 address of the outgoing interface and selected in accordance with RFC6724.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SYSLOG server.
Example
The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface-ipv6 vlan 100
```

22.5 logging console
Use the logging console Global Configuration mode command to limit messages logged to the console to messages to a specific severity level. Use the no form of this command to restore the default.

Syntax
```
logging console level
no logging console
```

Parameters
- **level**—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration
Informational.

Command Mode
Global Configuration mode

Example
The following example limits logging messages displayed on the console to messages with severity level errors.

```
switchxxxxxx(config)# logging console errors
```

22.6 logging buffered
Use the logging buffered Global Configuration mode command to limit the SYSLOG message display to messages with a specific severity level, and to
define the buffer size (number of messages that can be stored). Use the no form of this command to cancel displaying the SYSLOG messages, and to return the buffer size to default.

Syntax

logging buffered [buffer-size] [severity-level | severity-level-name]

no logging buffered

Parameters

- **buffer-size**—Specifies the maximum number of messages stored in the history table. (Range: 20–1000)
- **severity-level**—Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is informational.

The default buffer size is 200.

Command Mode

Global Configuration mode

User Guidelines

All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level debugging. In the second example, the buffer size is set to 100.

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 7
```
22.7 clear logging

Use the clear logging Privileged EXEC mode command to clear messages from the internal logging buffer.

Syntax

clear logging

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

switchxxxxxx# clear logging
Clear logging buffer [confirm]

22.8 logging file

Use the logging file Global Configuration mode command to limit SYSLOG messages sent to the logging file to messages with a specific severity level. Use the no form of this command to cancel sending messages to the file.

Syntax

logging file level

no logging file
Parameters

level—Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is errors.

Command Mode

Global Configuration mode

Example

The following example limits SYSLOG messages sent to the logging file to messages with severity level alerts.

```
switchxxxxxx(config)# logging file alerts
```

### 22.9 clear logging file

Use the `clear logging file` Privileged EXEC mode command to clear messages from the logging file.

Syntax

```
clear logging file
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode
Example

The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
```

Clear Logging File [y/n]

22.10 aaa logging

Use the `aaa logging` Global Configuration mode command to enable logging AAA logins. Use the `no` form of this command to disable logging AAA logins.

Syntax

```
aaa logging {login}
no aaa logging {login}
```

Parameters

`login`—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

Example

The following example enables logging AAA login events.

```
switchxxxxxx(config)# aaa logging login
```
22.11 file-system logging

Use the file-system logging Global Configuration mode command to enable logging file system events. Use the no form of this command to disable logging file system events.

Syntax

file-system logging {copy | delete-rename}

no file-system logging {copy | delete-rename}

Parameters

- copy—Specifies logging messages related to file copy operations.
- delete-rename—Specifies logging messages related to file deletion and renaming operations.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging messages related to file copy operations.

```
switchxxxxxxx(config)# file-system logging copy
```

22.12 logging aggregation on

Use the logging aggregation on Global Configuration mode command to control aggregation of SYSLOG messages. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by logging aggregation aging-time). Use the no form of this command to disable aggregation of SYSLOG messages.

Syntax

logging aggregation on
no logging aggregation on

Parameters
N/A

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

### 22.13 logging aggregation aging-time

Use the `logging aggregation aging-time` Global Configuration mode command to configure the aging time of the aggregated SYSLOG messages. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. Use the `no` form of this command to return to the default.

**Syntax**

```
logging aggregation aging-time sec
no logging aggregation aging-time
```

**Parameters**

- `aging-time sec`—Aging time in seconds (Range: 15–3600)

**Default Configuration**

300 seconds.

**Command Mode**

Global Configuration mode
### Example

```
switchxxxxxx(config)# logging aggregation aging-time 300
```

### 22.14 logging origin-id

Use the `logging origin-id` Global Configuration mode command to configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server. Use the `no` form of this command to return to the default.

**Syntax**

```
logging origin-id {hostname | IP | IPv6 | string user-defined-id}
no logging origin-id
```

**Parameters**

- `hostname`—The system hostname will be used as the message origin identifier.
- `IP`—IP address of the sending interface that is used as the message origin identifier.
- `IPv6`—IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- `string user-defined-id`—Specifies an identifying description chosen by the user. The `user-defined-id` argument is the identifying description string.

**Default Configuration**

No header is sent apart from the PRI field.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# logging origin-id string "Domain 1, router B"
```
22.15  show logging

Use the show logging Privileged EXEC mode command to display the logging status and SYSLOG messages stored in the internal buffer.

Syntax

show logging

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

```
switchxxxxxx# show logging
Logging is enabled.
Origin id: hostname
Console Logging: Level info. Console Messages: 0 Dropped.
4 messages were not logged
Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
Management ACL          Deny      Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up: Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down: SYSLOG8

### 22.16 show logging file

Use the `show logging file` Privileged EXEC mode command to display the logging status and the SYSLOG messages stored in the logging file.

**Syntax**

`show logging file`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the logging status and the SYSLOG messages stored in the logging file.

```
switchxxxxxx# show logging file
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
```
4 messages were not logged

Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Deny</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Aggregation: Disabled.
Aggregation aging time: 300 Sec

01-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob bgEgGnt9z6NHgwKI5xK$r7cBtd11xmFgSEWuDhho5UedydA$kJK55XR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 != SIGBLOB_LEN

22.17 show syslog-servers

Use the show syslog-servers Privileged EXEC mode command to display the SYSLOG server settings.

Syntax
show syslog-servers

Parameters
N/A
**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example provides information about the SYSLOG servers.

```
switchxxxxxx# show syslog-servers
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Device Configuration

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Facility</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.121</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td></td>
</tr>
<tr>
<td>3000::100</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td></td>
</tr>
</tbody>
</table>
```
Remote Network Monitoring (RMON) Commands

23.1 show rmon statistics

Use the `show rmon statistics` EXEC mode command to display RMON Ethernet statistics.

Syntax

```
show rmon statistics {interface-id}
```

Parameters

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays RMON Ethernet statistics for port gi1/1/1.

```
switchxxxxxx# show rmon statistics gi1/1/1
Port gi1/1/1
Dropped: 0
Octets: 0   Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 to 127 Octets: 1
128 to 255 Octets: 1  256 to 511 Octets: 1
512 to 1023 Octets: 0  1024 to max Octets: 0
```
The following table describes the significant fields displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped</td>
<td>Total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.</td>
</tr>
<tr>
<td>Octets</td>
<td>Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>Total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Total number of good packets received and directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions</td>
<td>Best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>64 Octets</td>
<td>Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
Remote Network Monitoring (RMON) Commands

23.2 rmon collection stats

Use the rmon collection stats Interface Configuration mode command to enable RMON MIB collecting history statistics (in groups) on an interface. Use the no form of this command to remove a specified RMON history group of statistics.

Syntax

rmon collection stats index [owner ownername] [buckets bucket-number] [interval seconds]

no rmon collection stats index

Parameters

- **index**—The requested group of statistics index.(Range: 1–65535)
- **owner ownername**—Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- **buckets bucket-number**—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50.(Range: 1–50)
- **interval seconds**—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description                                                                ABL</th>
</tr>
</thead>
<tbody>
<tr>
<td>65 to 127 Octets</td>
<td>Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255 Octets</td>
<td>Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256 to 511 Octets</td>
<td>Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512 to 1023 Octets</td>
<td>Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024 to max Octets</td>
<td>Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration (Ethernet, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

23.3 show rmon collection stats

Use the show rmon collection stats EXEC mode command to display the requested RMON history group statistics.

Syntax

show rmon collection stats [interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays all RMON history group statistics.

```
switchxxxxxx# show rmon collection stats
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
<th>Interval</th>
<th>Requested Samples</th>
<th>Granted Samples</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>gi1/1/1</td>
<td>30</td>
<td>50</td>
<td>50</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>gi1/1/1</td>
<td>1800</td>
<td>50</td>
<td>50</td>
<td>Manager</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The sampled Ethernet interface.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds between samples.</td>
</tr>
<tr>
<td>Requested Samples</td>
<td>The requested number of samples to be saved.</td>
</tr>
</tbody>
</table>
23.4 **show rmon history**

Use the `show rmon history` EXEC mode command to display RMON Ethernet history statistics.

**Syntax**

```
show rmon history index {throughput | errors | other} [period seconds]
```

**Parameters**

- **index**—Specifies the set of samples to display. (Range: 1–65535)
- **throughput**—Displays throughput counters.
- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period seconds**—Specifies the period of time in seconds to display. (Range: 1–2147483647)

**Command Mode**

EXEC mode

**Example**

The following examples display RMON Ethernet history statistics for index 1

```
switchxxxxxx# show rmon history 1 throughput
Sample Set: 1 Owner: CLI
Interface: gi1/1/1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500
Time Octets Packets Broadcast Multicast Util
----------------- ------- ------- --------- --------- ----
Jan 18 2005 21:57:00 303595962 357568 3289 7287 19%
Jan 18 2005 21:57:30 287696304 275686 2789 5878 20%
```
The following table describes significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and Time the entry is recorded.</td>
</tr>
<tr>
<td>Octets</td>
<td>Total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets (including bad packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Number of good packets received during this sampling interval that were directed to the broadcast address.</td>
</tr>
</tbody>
</table>
### 23.5 rmon alarm

Use the `rmon alarm` Global Configuration mode command to configure alarm conditions. Use the `no` form of this command to remove an alarm.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast</td>
<td>Number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>CRC Align</td>
<td>Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize</td>
<td>Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Oversize</td>
<td>Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for <code>etherHistoryFragments</code> to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Dropped</td>
<td>Total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.</td>
</tr>
<tr>
<td>Collisions</td>
<td>Best estimate of the total number of collisions on this Ethernet segment during this sampling interval.</td>
</tr>
</tbody>
</table>
**Syntax**

```
rmon alarm index mib-object-id interval rising-threshold falling-threshold rising-event falling-event [type {absolute | delta}] [startup {rising | rising-falling | falling}] [owner name]
```

**no rmon alarm index**

**Parameters**

- **index**—Specifies the alarm index. (Range: 1–65535)
- **mib-object-id**—Specifies the object identifier of the variable to be sampled. (Valid OID)
- **interval**—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–4294967295)
- **rising-threshold**—Specifies the rising threshold value. (Range: 0–4294967295)
- **falling-threshold**—Specifies the falling threshold value. (Range: 0–4294967295)
- **rising-event**—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- **falling-event**—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)
- **type {absolute | delta}**—Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - **absolute**—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - **delta**—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- **startup {rising | rising-falling | falling}**—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rising-threshold**, a single rising alarm is generated.
- **rising-falling**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rising-threshold**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.

- **falling** —Specifies that if the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.

  - **owner name**—Specifies the name of the person who configured this alarm. (Valid string)

Default Configuration

The default method type is **absolute**.

The default **startup** direction is **rising-falling**.

If the **owner name** is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
switchxxxxxx(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20
```

**23.6 show rmon alarm-table**

Use the **show rmon alarm-table** EXEC mode command to display a summary of the alarms table.

**Syntax**

```
show rmon alarm-table
```
**Command Mode**

EXEC mode

**Example**

The following example displays the alarms table.

```
switchxxxxxx# show rmon alarm-table
Index  OID          Owner
-----  ------------  -----
1      1.3.6.1.2.1.2.2.1.10.1  CLI
2      1.3.6.1.2.1.2.2.1.10.1  Manager
3      1.3.6.1.2.1.2.2.1.10.9   CLI
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

**23.7 show rmon alarm**

Use the `show rmon alarm` EXEC mode command to display alarm configuration.

**Syntax**

`show rmon alarm number`

**Parameters**

`alarm number`— Specifies the alarm index. (Range: 1–65535)

**Command Mode**

EXEC mode

**Example**

The following example displays RMON 1 alarms.
switchxxxxxx# show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Alarm index.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Last Sample Value</td>
<td>Value of the statistic during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.</td>
</tr>
<tr>
<td>Interval</td>
<td>Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>Method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is delta, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.</td>
</tr>
<tr>
<td>Startup Alarm</td>
<td>Alarm that is sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.</td>
</tr>
</tbody>
</table>
Remote Network Monitoring (RMON) Commands

23.8 rmon event

Use the `rmon event` Global Configuration mode command to configure an event. Use the `no` form of this command to remove an event.

Syntax

```
rmon event index {none | log | trap | log-trap} [community text] [description text] [owner name]
```

```
no rmon event index
```

Parameters

- `index`—Specifies the event index. (Range: 1–65535)
- `none`—Specifies that no notification is generated by the device for this event.
- `log`—Specifies that a notification entry is generated in the log table by the device for this event.
- `trap`—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
- `log-trap`—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- `community text`—Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string;...
Remote Network Monitoring (RMON) Commands

length: 0–127 characters). Note this must be a community used in the definition of an SNMP host using the “snmp-server host” command.

- **description text**—Specifies a comment describing this event. (Length: 0–127 characters)
- **owner name**—Specifies the name of the person who configured this event. (Valid string)

Default Configuration

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
switchxxxxxx(config)# rmon event 10 log
```

23.9  **show rmon events**

Use the **show rmon events** EXEC mode command to display the RMON event table.

Syntax

```
show rmon events
```

Command Mode

EXEC mode
Example

The following example displays the RMON event table.

```
switchxxxxxx# show rmon events
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Type</th>
<th>Community</th>
<th>Owner</th>
<th>Last time sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Errors</td>
<td>Log</td>
<td>router</td>
<td>CLI</td>
<td>Jan 18 2006 23:58:17</td>
</tr>
<tr>
<td>2</td>
<td>High Broadcast</td>
<td>Log</td>
<td>Manager</td>
<td></td>
<td>Jan 18 2006 23:59:48</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Unique index that identifies this event.</td>
</tr>
<tr>
<td>Description</td>
<td>Comment describing this event.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of notification that the device generates about this event.</td>
</tr>
<tr>
<td>Community</td>
<td>If an SNMP trap is to be sent, it is sent with the SNMP community string specified by this octet string.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this event.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The time this entry last generated an event. If this entry has not generated any events, this value is zero.</td>
</tr>
</tbody>
</table>

### 23.10 show rmon log

Use the `show rmon log` EXEC mode command to display the RMON log table.

**Syntax**

```
show rmon log [event]
```

**Parameters**

- **event**—Specifies the event index. (Range: 0–65535)
Example

The following example displays event 1 in the RMON log table.

```
switchxxxxxx# show rmon log 1
Maximum table size: 500 (800 after reset)
Event Description Time
----- -------------- ----------------
1 MIB Var.: 1.3.6.1.2.1.2.2.1.10.
     53, Delta, Rising, Actual Val: 800,
     Thres.Set: 100, Interval (sec): 1
```

23.11 rmon table-size

Use the `rmon table-size` Global Configuration mode command to configure the maximum size of RMON tables. Use the `no` form of this command to return to the default size.

Syntax

```
rmon table-size {history entries | log entries}
no rmon table-size {history | log}
```

Parameters

- `history entries`—Specifies the maximum number of history table entries. (Range: 20–270)
- `log entries`—Specifies the maximum number of log table entries. (Range: 20–100)

Default Configuration

The default history table size is 270 entries.
The default log table size is 200 entries.

Command Mode

Global Configuration mode
User Guidelines

The configured table size takes effect after the device is rebooted.

Example

The following example configures the maximum size of RMON history tables to 100 entries.

```
switchxxxxxx(config)# rmon table-size history 100
```
802.1X Commands

Dependencies Between Multi-Session Mode and System Mode

Multi-session mode works differently in Switch (L2) system mode and Router (L3) system mode, as described below:

- **Switch system mode**—Guest VLAN, RADIUS VLAN attributes are supported in Sx500 devices. For SG500X and SG500XG devices, these features are always supported.

- **Router system mode**—Guest VLAN and RADIUS VLAN attributes are not supported for Sx500 devices. They are supported for SG500X and SG500XG devices.

List of Commands

24.1 aaa authentication dot1x

Use the `aaa authentication dot1x` Global Configuration mode command to specify which servers are used for authentication when 802.1X authentication is enabled. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
aaa authentication dot1x default {radius | none | {radius | none}}
no aaa authentication dot1x default
```

**Parameters**

- **radius** - Uses the list of all RADIUS servers for authentication
- **none** - Uses no authentication

**Default Configuration**

RADIUS server.
Command Mode
Global Configuration mode

User Guidelines
You can select either authentication by a RADIUS server, no authentication (none), or both methods.

If you require that authentication succeeds even if no RADIUS server response was received, specify none as the final method in the command line.

Example
The following example sets the 802.1X authentication mode to RADIUS server authentication. Even if no response was received, authentication succeeds.

```
switchxxxxxxx(config)# aaa authentication dot1x default radius none
```

### 24.2 clear dot1x statistics

Use the `clear dot1x statistics` Privileged EXEC mode command to clear 802.1X statistics.

Syntax
```
clear dot1x statistics [interface-id]
```

Parameters
- `interface-id`—Specify an Ethernet port ID.

Default Configuration
Statistics on all ports are cleared.

Command Mode
Privileged EXEC

User Guidelines
This command clears all the counters displayed in the `show dot1x` and `show dot1x statistics` command.
Example

```
switchxxxxxx# clear dot1x statistics
```

### 24.3 data

To specify web-based page customization, the `data` command in Web-Based Page Customization Configuration mode is used.

**Syntax**

```
data value
```

**Parameters**

- `value`—String of hexadecimal digit characters up to 320 characters.

**Default Configuration**

No user customization.

**Command Mode**

Web-Based Page Customization Configuration mode

**User Guidelines**

The command should not be entered or edited manually (unless using copy-paste). It is a part of the configuration file produced by the switch.

A user can only customize the web-based authentication pages by using the WEB interface.

**Examples**

**Example 1**—The following example shows a partial web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

Example 2—The following example shows how Web-Based Page customization is displayed when running the `show running-config` command:

```
switchxxxxx# show running-config
.
.
.
dot1x page customization
data ********
exit
.
.
.
```

### 24.4 dot1x auth-not-req

Use the `dot1x auth-not-req` Interface Configuration (VLAN) mode command to enable unauthorized devices access to a VLAN. Use the `no` form of this command to disable access to a VLAN.

**Syntax**

- `dot1x auth-not-req`
- `no dot1x auth-not-req`

**Parameters**

N/A

**Default Configuration**

Access is enabled.

**Command Mode**

Interface Configuration (VLAN) mode
User Guidelines

A VLAN cannot be defined as an unauthenticated VLAN if it is an access VLAN or it is the native VLAN for some ports.

If a VLAN is configured as an unauthenticated VLAN, traffic tagged with that VLAN and received from a member port of that VLAN will be bridged regardless of whether the port/host is authorized or not.

The guest VLAN cannot be configured as unauthorized VLAN.

Example

The following example enables unauthorized devices access to VLAN 5.

```bash
switchxxxxxx(config)# interface vlan 5
switchxxxxxx(config-if)# dot1x auth-not-req
```

24.5 dot1x authentication

Use the `dot1x authentication` Interface Configuration mode command to enable authentication methods on a port. Use the `no` format of the command to return to the default.

Syntax

```
don1x authentication [802.1x] [mac] [web]
no dot1x authentication
```

Parameters

- **802.1x**—Enables authentication based on 802.1X (802.1X-based authentication).
- **mac**—Enables authentication based on the station's MAC address (MAC-Based authentication).
- **web**—Enables WEB-Based authentication.

Default Configuration

802.1X-Based authentication is enabled.
Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Static MAC addresses cannot be authorized by the MAC-based method.

It is not recommended to change a dynamic MAC address to a static one or delete it if the MAC address was authorized by the MAC-based authentication:

a. If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated.

b. Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.

The WEB-Based authentication is supported only when the device is configured to switch (L2) system mode.

Example

The following example enables authentication based on 802.1x and the station’s MAC address on port gi1:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

24.6 dot1x guest-vlan

Use the dot1x guest-vlan Interface Configuration (VLAN) mode command to define a guest VLAN. Use the no form of this command to restore the default configuration.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Parameters

N/A
Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the `dot1x guest-vlan enable` command to enable unauthorized users on an interface to access the guest VLAN.

A device can have only one global guest VLAN.

The guest VLAN must be a static VLAN and it cannot be removed.

An unauthorized VLAN cannot be configured as guest VLAN.

The guest VLAN cannot be configured on a monitoring port. See Dependencies Between Multi-Session Mode and System Mode

Example

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

### 24.7 dot1x guest-vlan enable

Use the `dot1x guest-vlan enable` Interface Configuration mode command to enable unauthorized users on the access interface to the guest VLAN. Use the `no` form of this command to disable access.

Syntax

```
dot1x guest-vlan enable
no dot1x guest-vlan enable
```

Parameters

N/A
Default Configuration
The default configuration is disabled.

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
The port cannot belong to the guest VLAN.

See [Dependencies Between Multi-Session Mode and System Mode](#) for more information about the guest VLAN.

The guest VLAN and the WEB-Based authentication cannot be configured on a port at the same time.

The port is added to the guest VLAN as an egress untagged port.

If the authentication mode is single-host or multi-host, the value of PVID is set to the guest VLAN_ID.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs from unauthorized hosts are mapped to the guest VLAN.

If 802.1X is disabled, the port static configuration is reset.

If the guest VLAN is disabled on the port its static configuration is reset.

See the User Guidelines of the `dot1x host-mode` command for more information.

Example
The following example enables unauthorized users on `gi1/1/1` to access the guest VLAN.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

### 24.8 dot1x guest-vlan timeout

Use the `dot1x guest-vlan timeout` Global Configuration mode command to set the time delay between enabling 802.1X (or port up) and adding a port to the guest VLAN. Use the `no` form of this command to restore the default configuration.
24.9  dot1x host-mode

Use the dot1x host-mode Interface Configuration mode command to allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port. Use the no form of this command to return to the default setting.

Syntax

dot1x host-mode [multi-host | single-host | multi-sessions]

Parameters

- multi-host—Enable multiple-hosts mode.
- **single-host**—Enable single-hosts mode.
- **multi-sessions**—Enable multiple-sessions mode.

**Default Configuration**
Default mode is multi-host.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**

**Single-Host Mode**
The single-host mode manages the authentication status of the port: the port is authorized if there is an authorized host. In this mode, only a single host can be authorized on the port.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static vlan membership configured at the port. Traffic from other hosts is dropped.

A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS-assigned VLAN or the unauthenticated VLANs. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

**Multi-Host Mode**
The multi-host mode manages the authentication status of the port: the port is authorized after at least one host is authorized.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged based on the static vlan membership configured at the port.

A user can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the
authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS assigned VLAN or the unauthenticated VLANs. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

**Multi-Sessions Mode**

Unlike the single-host and multi-host modes (port-based modes) the multi-sessions mode manages the authentication status for each host connected to the port (session-based mode). If the multi-sessions mode is configured on a port the port does have any authentication status. Any number of hosts can be authorized on the port. The `dot1x max-hosts` command can limit the maximum number of authorized hosts allowed on the port.

See [Dependencies Between Multi-Session Mode and System Mode](#) for more information about the multi-sessions mode.

In Switch system mode each authorized client requires a TCAM rule. If there is no available space in the TCAM, the authentication is rejected. When using the `dot1x host-mode` command to change the port mode to `single-host` or `multi-host` when authentication is enabled, the port state is set to unauthorized.

If the `dot1x host-mode` command changes the port mode to `multi-session` when authentication is enabled, the state of all attached hosts is set to unauthorized.

To change the port mode to single-host or multi-host, set the port (`dot1x port-control`) to force-unauthorized, change the port mode to single-host or multi-host, and set the port to authorization auto.

Tagged traffic belonging to the unauthenticated VLANs is always bridged regardless if a host is authorized or not.

When the guest VLAN is enabled, untagged and tagged traffic from unauthorized hosts not belonging to the unauthenticated VLANs is bridged via the guest VLAN.

Traffic from an authorized hosts is bridged in accordance with the port static configuration. A user can specify that untagged and tagged traffic from the authorized host not belonging to the unauthenticated VLANs will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

When TCAM is used, the multi-sessions mode cannot be configured on the same interface together with Policy Based VLANs configured by the following commands:

- `switchport general map protocols-group vlan`
- `switchport general map macs-group vlan`
Example

switchxxxxxx(config)# interface gi1/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
switchxxxxxx(config-if)# dot1x host-mode single-host
switchxxxxxx(config-if)# dot1x host-mode multi-sessions

24.10  dot1x max-hosts

Use the dot1x max-hosts interface configuration command to configure the maximum number of authorized hosts allowed on the interface. Use the no format of the command to return to the default.

Syntax

dot1x max-hosts count
no dot1x max-hosts

Parameters

count—Specifies the maximum number of authorized hosts allowed on the interface. May be any 32 bits positive number.

Default Configuration

No limitation.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

By default, the number of authorized hosts allowed on an interface is not limited. To limit the number of authorized hosts allowed on an interface, use the dot1x max-hosts command.

This command is relevant only for multi-session mode.
Example
The following example limits the maximum number of authorized hosts on Ethernet port gi25 to 6:

```
switchxxxxxx(config)# interface gi1/1/25
switchxxxxxx(config-if)# dot1x max-hosts 6
```

24.11 dot1x max-login-attempts
To set the maximum number of allowed login attempts, use this command in Interface Configuration mode. To return to the default setting, use the no form of this command.

Syntax
```
dot1x max-login-attempts count
no dot1x max-login-attempts
```

Parameters
- `count`— Specifies the maximum number of allowed login attempts. A value of 0 means an infinite numbers of attempts. The valid range is 3-10.

Default Configuration
Unlimited.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
By default, the switch does not limit the number of failed login attempts. To specify the number of allowed fail login attempts, use this command. After this number of failed login attempts, the switch does not allow the host to be authenticated for a period defined by the `dot1x timeout quiet-period` command.

The command is applied only to the Web-based authentication.
Example

The following example sets maximum number of allowed login attempts to 5:

```
switchxxxxx(config)# interface gi15
switchxxxxx(config-if)# dot1x max-login-attempts 5
```

### 24.12 dot1x max-req

Use the `dot1x max-req` Interface Configuration mode command to set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
dot1x max-req count
no dot1x max-req
```

**Parameters**

- `max-req count`—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10)

**Default Configuration**

The default maximum number of attempts is 2.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.
Example

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6.

```
switchxxxxxx(config)# interface gi1/15
switchxxxxxx(config-if)# dot1x max-req 6
```

### 24.13 dot1x page customization

Use the `dot1x page customization` command in Global Configuration mode command to enter the Web-Based Page Customization Configuration mode.

**Syntax**

```
dot1x page customization
```

**Parameters**

N/A

**Default Configuration**

No user customization.

**Command Mode**

Global Configuration mode

**User Guidelines**

The command should not be entered or edited manually (unless when using copy-paste). It is a part of the configuration file produced by the switch.

A user must customize the web-based authentication pages by using the browser interface.

**Example**

The following example shows part of a web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
```
24.14 dot1x port-control

Use the dot1x port-control Interface Configuration mode command to enable manual control of the port authorization state. Use the no form of this command to restore the default configuration.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}[time-range time-range-name]

Parameters

- **auto**—Enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.

- **force-authorized**—Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives traffic without 802.1X-based client authentication.

- **force-unauthorized**—Denies all access through this port by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through this port.

- **time-range time-range-name**— Specifies a time range. When the Time Range is not in effect, the port state is Unauthorized. (Range: 1-32 characters).

Default Configuration

The port is in the force-authorized state.

Command Mode

Interface Configuration (Ethernet) mode
User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge ports (ports in auto state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example sets 802.1X authentication on gi15 to auto mode.

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x port-control auto
```

24.15 dot1x radius-attributes vlan

Use the dot1x radius-attributes vlan Interface Configuration mode command to enable RADIUS-based VLAN assignment. Use the no form of this command to disable RADIUS-based VLAN assignment.

Syntax

dot1x radius-attributes vlan [reject | static]
no dot1x radius-attributes vlan

Parameters

- **reject**— If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN the supplicant is rejected. If the parameter is omitted, this option is applied by default.

- **static**— If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

Default Configuration

reject

Command Mode

Interface Configuration (Ethernet) mode
User Guidelines

The command is not supported when the system is in Router system mode. See Dependencies Between Multi-Session Mode and System Mode.

If RADIUS provides invalid VLAN information, the authentication is rejected.

If a RADIUS server assigns a client with a non-existing VLAN, the switch creates the VLAN. The VLAN is removed when it is no longer being used.

If RADIUS provides valid VLAN information and the port does not belong to the VLAN received from RADIUS, it is added to the VLAN as an egress untagged port. When the last authorized client assigned to the VLAN becomes unauthorized or 802.1x is disabled on the port, the port is excluded from the VLAN.

If the authentication mode is single-host or multi-host, the value of PVID is set to the VLAN_ID.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs are mapped to the VLAN using TCAM. See the User Guidelines of the `dot1x host-mode` command for more information.

If 802.1X is disabled the port static configuration is reset.

If an authorized port in the single-host or multi-host mode changes its status to unauthorized, the port static configuration is reset.

If the last authorized host assigned to a VLAN received from RADIUS connected to a port in the multi-sessions mode changes its status to unauthorized, the port is removed from the VLAN if it is not in the static configuration.

If the `reject` keyword is configured and the RADIUS server authorizes the host but the RADIUS accept message does not assign a VLAN to the supplicant, authentication is rejected.

If the `static` keyword is configured and the RADIUS server authorizes the host then even though the RADIUS accept message does not assign a VLAN to the supplicant, authentication is accepted and the traffic from the host is bridged in accordance with port static configuration.

If this command is used when there are authorized ports/hosts, it takes effect at subsequent authentications. To manually re-authenticate, use the `dot1x re-authenticate` command.
Example

Example 1. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant but did not provide a supplicant VLAN, the supplicant is accepted and the static VLAN configurations is used.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x radius-attributes static
switchxxxxxx(config-if)# exit
```

24.16 dot1x re-authenticate

The `dot1x re-authenticate` Privileged EXEC mode command manually initiates re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

Syntax

`dot1x re-authenticate [interface-id]`

Parameters

`interface-id`—Specifies an Ethernet port.

Default Configuration

If no port is specified, command is applied to all ports.

Command Mode

Privileged EXEC mode
Example
The following command manually initiates re-authentication of 802.1X-enabled gi15:

switchxxxxxx# dot1x re-authenticate gi1/15

24.17 dot1x reauthentication
Use the dot1x reauthentication Interface Configuration mode command to enable periodic re-authentication of the client. Use the no form of this command to return to the default setting.

Syntax

dot1x reauthentication  
no dot1x reauthentication

Parameters
N/A

Default Configuration
Periodic re-authentication is disabled.

Command Mode
Interface configuration (Ethernet)

Example

switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x reauthentication

24.18 dot1x system-auth-control
Use the dot1x system-auth-control Global Configuration mode command to enable 802.1X globally. Use the no form of this command to restore the default configuration.
Syntax

dot1x system-auth-control

no dot1x system-auth-control

Parameters

N/A

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables 802.1X globally.

switchxxxxxx(config)# dot1x system-auth-control

24.19  dot1x timeout quiet-period

Use the dot1x timeout quiet-period Interface Configuration mode command to set the time interval that the device remains in a quiet state following a failed authentication exchange (for example, if the client provided an invalid password).

For 802.1x and MAC-based authentication, the number of failed logins is 1. For web-based authentication, the number of failed attempts is configured by the dot1x max-login-attempts command.

Use the no form of this command to restore the default configuration.

Syntax

dot1x timeout quiet-period seconds

no dot1x timeout quiet-period
Parameters

seconds—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with a client. (Range: 10–65535 seconds)

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

For WEB-based authentication, the quite period is applied after a number of failed attempts. This number is configured by the dot1x max-login-attempts command.

For 802.1x-based and MAC-based authentication methods, the quite period is applied after each failed attempt.

Example

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 120 seconds.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

24.20 dot1x timeout reauth-period

Use the dot1x timeout reauth-period Interface Configuration mode command to set the number of seconds between re-authentication attempts. Use the no form of this command to return to the default setting.
802.1X Commands

24 802.1X Commands

Syntax

dot1x timeout reauth-period seconds
no dot1x timeout reauth-period

Parameters

reauth-period seconds—Number of seconds between re-authentication attempts. (Range: 300-4294967295)

Default Configuration

3600

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command is only applied to the 802.1x authentication method.

Example

switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000

24.21 dot1x timeout server-timeout

Use the dot1x timeout server-timeout Interface Configuration mode command to set the time interval during which the device waits for a response from the authentication server. Use the no form of this command to restore the default configuration.

Syntax

dot1x timeout server-timeout seconds
no dot1x timeout server-timeout

Parameters

server-timeout seconds—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds)
Default Configuration
The default timeout period is 30 seconds.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
The actual timeout period can be determined by comparing the value specified by this command to the result of multiplying the number of retries specified by the `radius-server retransmit` command by the timeout period specified by the `radius-server retransmit` command, and selecting the lower of the two values.

Example
The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

### 24.22 dot1x timeout silence-period
To set the authentication silence time, use the `dot1x timeout silence-period` command in Interface Configuration mode. The silence time is the number of seconds that if an authorized client does not send traffic during this period, the client is changed to unauthorized.

To return to the default setting, use the `no` form of this command.

**Syntax**

```
dot1x timeout silence-period seconds
no dot1x timeout silence-period
```

**Parameters**

- `seconds`— Specifies the silence interval in seconds. The valid range is 60 - 65535.

**Default Configuration**
The silence period is not limited.
Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command is only applied to WEB-based authentication.

If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.

Example

The following example sets the authentication silence time to 100 seconds:

```
dot1x timeout silence-period 100
```

24.23  dot1x timeout supp-timeout

Use the `dot1x timeout supp-timeout` Interface Configuration mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request. Use the `no` form of this command to restore the default configuration.

Syntax

```
dot1x timeout supp-timeout seconds

no dot1x timeout supp-timeout
```

Parameters

`supp-timeout seconds`—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode
User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

24.24 dot1x timeout tx-period

Use the `dot1x timeout tx-period` Interface Configuration mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request. Use the `no` form of this command to restore the default configuration.

Syntax

```
dot1x timeout tx-period seconds
no dot1x timeout tx-period
```

Parameters

```
seconds—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30–65535 seconds)
```

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode
User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds.

```
switchxxxxxx(config)# interface gi15:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

24.25 dot1x traps authentication failure

Use the `dot1x traps authentication failure` Global Configuration mode command to enable sending traps when an 802.1X authentication method failed. Use the `no` form of this command to return to the default.

Syntax

```
dot1x traps authentication failure {[802.1x] [mac] [web]}
no dot1x traps authentication failure
```

Parameters

- `802.1x`— Enables traps for 802.1X-based authentication.
- `mac`— Enables traps for MAC-based authentication.
- `web`— Enables traps for WEB-based authentication.

Default Configuration

All traps are disabled.

Command Mode

Global Configuration mode
**User Guidelines**

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

**Example**

The following example enables sending traps when a MAC address fails to be authorized by the 802.1X mac-authentication access control.

```
switchxxxxxx(config)#dot1x traps authentication failure mac
```

**24.26 dot1x traps authentication quiet**

Use the `dot1x traps authentication quiet` Global Configuration mode command to enable sending traps when a host state is set to the quiet state after failing the maximum sequential attempts of login. Use the `no` form of this command to disable the traps.

**Syntax**

```
dot1x traps authentication quiet
no dot1x traps authentication quiet
```

**Parameters**

N/A

**Default Configuration**

Quiet traps are disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

The traps are sent after the client is set to the quiet state after the maximum sequential attempts of login.

The command is only applied to the web-based authentication.
A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example
The following example enables sending traps when a host is set in the quiet state:

```
switchxxxxxx(config)#dot1x traps authentication quiet
```

24.27 dot1x traps authentication success

Use the dot1x traps authentication success Global Configuration mode command to enable sending traps when a host is successfully authorized by an 802.1X authentication method. Use the no form of this command to disable the traps.

Syntax

```
dot1x traps authentication success {[802.1x] [mac] [web]}
no dot1x traps authentication success
```

Parameters

- 802.1x— Enables traps for 802.1X-based authentication.
- mac— Enables traps for MAC-based authentication.
- web— Enables traps for WEB-based authentication.

Default Configuration
Success traps are disabled.

Command Mode
Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.
Example

The following example enables sending traps when a MAC address is successfully authorized by the 802.1X MAC-authentication access control.

```
switchxxxxx(config)#dot1x traps authentication success mac
```

### 24.28 dot1x unlock client

Use the `dot1x unlock client` Privileged EXEC mode command to unlock a locked (in the silence interval) client.

**Syntax**

```
dot1x unlock client interface-id mac-address
```

**Parameters**

- `interface-id`— Interface ID where the client is connected to.
- `mac-address`— Client MAC address.

**Default Configuration**

The client is locked until the silence interval is over.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use this command to unlock a client that was locked after the maximum allowed authentication failed attempts and to end the silence period. If the client is not in the silence period, the command has no affect.

**Example**

```
switchxxxxx(config)# dot1x unlock client gi1/1/1 00:01:12:af:00:56
```
24.29  dot1x violation-mode

Use the dot1x violation-mode Interface Configuration mode command to configure the action to be taken when an unauthorized host on authorized port in single-host mode attempts to access the interface. Use the no form of this command to return to default.

Syntax

```
dot1x violation-mode {restrict /protect /shutdown} [traps seconds]
```

```
no dot1x violation-mode
```

Parameters

- **restrict**—Generates a trap when a station, whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source addresses are not learned.

- **protect**—Discard frames with source addresses that are not the supplicant address.

- **shutdown**—Discard frames with source addresses that are not the supplicant address and shutdown the port.

- **trap seconds** - Send SNMP traps, and specifies the minimum time between consecutive traps. If `seconds = 0` traps are disabled. If the parameter is not specified, it defaults to 1 second for the restrict mode and 0 for the other modes.

Default Configuration

Protect

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command is relevant only for single-host mode.

For BPDU messages whose MAC addresses are not the supplicant MAC address are not discarded in Protect mode.

BPDU message whose MAC addresses are not the supplicant MAC address cause a shutdown in Shutdown mode.
Example

switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x violation-mode protect

24.30 show dot1x

Use the show dot1x Privileged EXEC mode command to display the 802.1X interfaces or specified interface status.

Syntax

show dot1x [interface interface-id | detailed]

Parameters

- interface-id—Specify an Ethernet port.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

The following example displays authentication information for all interfaces of the switch supporting the full multi-sessions mode:

switchxxxxxx# show dot1x

Authentication is enabled

Authenticating Servers: Radius, None

Unauthenticated VLANs: 100, 1000, 1021

Guest VLAN: VLAN 11, timeout 30 sec

Authentication failure traps are enables for 802.1x+mac

Authentication success traps are enables for 802.1x

Authentication quiet traps are enables for 802.1x
Gigaethernet 1/0/1

Host mode: multi-sessions
Authentication methods: 802.1x+mac
Port Adminstrated status: auto
Guest VLAN: enabled
VLAN Radius Attribute: enabled, static
Time range name: work_hours (Active now)
Server-timeout: 30 sec
Maximum Hosts: unlimited
Maximum Login Attempts: 3
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
   Tx period: 30 sec
      Supplicant timeout: 30 sec
         max-req: 2
Authentication success: 9
Authentication fails: 1
Number of Authorized Hosts: 10

Gigaethernet 1/0/2

Host mode: single-host
Authentication methods: 802.1x+mac
Port Adminstrated status: auto
Port Operational status: authorized
Guest VLAN: disabled
VLAN Radius Attribute: enabled
Time range name: work_hours (Active now)
Server-timeout: 30 sec
Aplied Authenticating Server: Radius
Applied Authentication method: 802.1x
Session Time (HH:MM:SS): 00:25:22
MAC Address: 00:08:78:32:98:66
Username: Bob
Violation:
  Mode: restrict
  Trap: enabled
  Trap Min Interval: 20 sec
  Violations were detected: 9
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
  Authentication success: 2
  Authentication fails: 0
GigaEthernet 1/0/3
  Host mode: single-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
MAC Address: 00:08:78:32:98:66
Username: Bob
Violation:
  Mode: restrict
  Trap: enabled
  Trap Min Interval: 20 sec
  Violations were detected: 0
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
Authentication success: 20
Authentication fails: 0

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>The port number.</td>
</tr>
<tr>
<td><strong>Host mode</strong></td>
<td>The port authentication configured mode. Possible values: single-host, multi-host, multi-sessions.</td>
</tr>
<tr>
<td><strong>Authentication methods</strong></td>
<td>Authentication methods configured on port. Possible values are combinations of the following methods: 802.1x, mac, or wba.</td>
</tr>
<tr>
<td><strong>Port Adminstrated status</strong></td>
<td>The port administration (configured) mode. Possible values: force-auth, force-unauth, auto.</td>
</tr>
<tr>
<td><strong>Port Operational status: authorized</strong></td>
<td>The port operational (actual) mode. Possible values: authorized or unauthorized.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>Username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authorized successfully.</td>
</tr>
<tr>
<td>Quiet period</td>
<td>Number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).</td>
</tr>
<tr>
<td>Silence period</td>
<td>Number of seconds that if an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.</td>
</tr>
<tr>
<td>Tx period</td>
<td>Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.</td>
</tr>
<tr>
<td>Max req</td>
<td>Maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.</td>
</tr>
<tr>
<td>Supplicant timeout</td>
<td>Number of seconds that the device waits for a response to an EAP-request frame from the client before resending the request.</td>
</tr>
<tr>
<td>Server timeout</td>
<td>Number of seconds that the device waits for a response from the authentication server before resending the request.</td>
</tr>
<tr>
<td>Session Time</td>
<td>Amount of time (HH:MM:SS) that the user is logged in.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Supplicant MAC address.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Authentication method used to establish the session.</td>
</tr>
<tr>
<td>Authentication success</td>
<td>Number of times the state machine received a Success message from the Authentication Server.</td>
</tr>
<tr>
<td>Authentication fails</td>
<td>Number of times the state machine received a Failure message from the Authentication Server.</td>
</tr>
</tbody>
</table>
### 24.31 show dot1x locked clients

Use the `show dot1x locked clients` Privileged EXEC mode command to display all clients who are locked and in the silence period.

**Syntax**

```
show dot1x locked clients
```

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use the `show dot1x locked clients` command to display all locked (in the silence period clients).

**Examples** The following example displays locked clients:

**Example 1**

```
switchxxxxxx# show dot1x locked clients
Port      MAC Address     Remaining Time
-------   ------------    ------------
gil/1/1    0008.3b79.8787      20
gil/1/1    0008.3b89.3128      40
gil/1/1       0008.3b89.3129      10
```

### 24.32 show dot1x statistics

Use the `show dot1x statistics` Privileged EXEC mode command to display 802.1X statistics for the specified port.

**Syntax**

```
show dot1x statistics interface interface-id
```

**Example**

```
switchxxxxxx# show dot1x statistics interface gil/1/1
```

**Port Statistics**

```
Port Statistics for gil/1/1

Octets                     Frames
Gil/1/1                     1234
```

**Octets**

```
Octets: 1234
```

**Frames**

```
Frames: 5678
```

**Errors**

```
Errors: 90
```

**Clear-Counters**

```
Clear-Counters: 10
```
Parameters

interface-id—Specifies an Ethernet port ID.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1X statistics for gi1/1/1.

```
switchxxxxxx# show dot1x statistics interface gi1/1/1
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```
The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EapolFramesRx</td>
<td>Number of valid EAPOL frames of any type that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolFramesTx</td>
<td>Number of EAPOL frames of any type that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolStartFramesRx</td>
<td>Number of EAPOL Start frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolLogoffFramesRx</td>
<td>Number of EAPOL Logoff frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespIdFramesRx</td>
<td>Number of EAP Resp/Id frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespFramesRx</td>
<td>Number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqIdFramesTx</td>
<td>Number of EAP Req/Id frames that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqFramesTx</td>
<td>Number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>InvalidEapolFramesRx</td>
<td>Number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.</td>
</tr>
<tr>
<td>EapLengthErrorFramesRx</td>
<td>Number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.</td>
</tr>
<tr>
<td>LastEapolFrameVersion</td>
<td>Protocol version number carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>LastEapolFrameSource</td>
<td>Source MAC address carried in the most recently received EAPOL frame.</td>
</tr>
</tbody>
</table>

### 24.33 show dot1x users

Use the `show dot1x users` Privileged EXEC mode command to display active 802.1X authorized users for the device.
Syntax

show dot1x users [username username]

Parameters

username—Specifies the supplicant username (Length: 1–160 characters)

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>Address</th>
<th>Method</th>
<th>Server</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa4/2/1</td>
<td>ccef485cb59d cc:ef:48:5c:b5:9d</td>
<td>MAC</td>
<td>Remote</td>
<td>02:06:03</td>
<td></td>
</tr>
<tr>
<td>fa4/2/2</td>
<td>7081053e0ee5 70:81:05:3e:0e:e5</td>
<td>MAC</td>
<td>Remote</td>
<td>02:06:03</td>
<td></td>
</tr>
<tr>
<td>fa4/2/3</td>
<td>c89c1d6e3d4d c8:9c:1d:6e:3d:4d</td>
<td>MAC</td>
<td>Remote</td>
<td>02:06:01</td>
<td></td>
</tr>
<tr>
<td>fa4/2/4</td>
<td>000e08d10adc 00:0e:08:d1:0a:dc</td>
<td>MAC</td>
<td>Remote</td>
<td>02:06:23</td>
<td></td>
</tr>
<tr>
<td>fa4/2/5</td>
<td>7081053dd137 70:81:05:3d:d1:37</td>
<td>MAC</td>
<td>Remote</td>
<td>02:06:00</td>
<td></td>
</tr>
<tr>
<td>fa4/2/6</td>
<td>7081053dd358 70:81:05:3d:d3:58</td>
<td>MAC</td>
<td>Remote</td>
<td>02:05:59</td>
<td></td>
</tr>
<tr>
<td>fa4/2/7</td>
<td>camera 00:21:29:72:82:da</td>
<td>802.1X</td>
<td>Remote</td>
<td>02:06:09</td>
<td></td>
</tr>
</tbody>
</table>
25.1  **interface**

Use the `interface` Global Configuration mode command to enter Interface configuration mode in order to configure an interface.

**Syntax**

```
interface interface-id
```

**Parameters**

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel, VLAN, range, IP interface or tunnel.

**Default Configuration**

N/A

**Command Mode**

Interface Configuration (Ethernet, port-channel, VLAN, range, IP interface or tunnel) mode

**Examples**

**Example 1**—For Gigabit Ethernet ports:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)#
```

**Example 2**—For Fast Ethernet ports:

```
switchxxxxxx(config)# interface fa1
switchxxxxxx(config-if)#
```
Example 3—For port channels (LAGs):

```
switchxxxxxx(config)# interface pol
switchxxxxxx(config-if)#
```

25.2 interface range

Use the `interface range` command to execute a command on multiple ports at the same time.

Syntax

```
interface range interface-id-list
```

Parameters

`interface-id-list`—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port, VLAN, or port-channel

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port-channel, or VLAN) mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Up to 255 characters can be used.

Example

```
switchxxxxxx(config)# interface range gi1/1/1-20
switchxxxxxx(config-if-range)#
```
25.3 shutdown

Use the `shutdown` Interface Configuration mode command to disable an interface. Use the `no` form of this command to restart a disabled interface.

**Syntax**

`shutdown`

`no shutdown`

**Parameters**

N/A

**Default Configuration**

The interface is enabled.

**Command Mode**

Interface Configuration mode

**User Guidelines**

The `shutdown` command sets a value of ifAdminStatus (see RFC 2863) to DOWN. When ifAdminStatus is changed to DOWN, ifOperStatus will also be changed to DOWN.

The DOWN state of ifOperStatus means that the interface does not transmit/receive messages from/to higher levels. For example, if you shut down a VLAN, on which an IP interface is configured, bridging into the VLAN continues, but the switch cannot transmit and receive IP traffic on the VLAN.

**Notes:**

- If the switch shuts down an Ethernet port it additionally shuts down the port MAC sublayer too.
- If the switch shuts down a port channel it additionally shuts down all ports of the port channel too.

**Example**

**Example 1**—The following example disables gi1/1/5 operations.

```
switchxxxxxx(config)# interface gi1/1/5
```
Example 2—The following example restarts the disabled Ethernet port.

```
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 3—The following example shuts down vlan 100.

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)
```

Example 4—The following example shuts down tunnel 1.

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)
```

Example 5—The following example shuts down Port Channel 3.

```
switchxxxxxx(config)# interface po3
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)
```

25.4 operation time

Use the operation time Interface Configuration (Ethernet) mode command to control the time that the port is up. Use the no form of this command to cancel the time range for the port operation time.
Syntax

operation time time-range-name
no operation time

Parameters

- time-range-name—Specifies a time range the port operates (in up state). When the Time Range is not in effect, the port is shutdown. (Range: 1–32 characters)

Default Configuration

There is no time range configured on the port authorized state.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The operation time command influences the port if the port status is up. This command defines the time frame during which the port stays up and at which time the port will be shutdown. While the port is in shutdown because of other reasons, this command has no effect.

The following example activates an operation time range (named "morning") on port gi1/1/15.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# operation time morning
```

25.5 description

Use the description Interface Configuration (Ethernet, port-channel) mode command to add a description to an interface. Use the no form of this command to remove the description.
25.6  speed

Use the `speed` Interface Configuration (Ethernet, port-channel) mode command to configure the speed of a given Ethernet interface when not using auto-negotiation. Use the `no` form of this command to restore the default configuration.

Syntax

```
speed {10 | 100 | 1000 | 10000}
```

Parameters

- **10**—Forces 10 Mbps operation
- **100**—Forces 100 Mbps operation
- **1000**—Forces 1000 Mbps operation

Example

The following example adds the description 'SW#3' to gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# description SW#3
```
### Ethernet Configuration Commands

**10000**—Forces 10000 Mbps operation

**Default Configuration**

The port operates at its maximum speed capability.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

The `no speed` command in a port-channel context returns each port in the port-channel to its maximum capability.

**Example**

The following example configures the speed of gi1/1/5 to 100 Mbps operation.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# speed 100
```

### 25.7 duplex

Use the `duplex` Interface Configuration (Ethernet, port-channel) mode command to configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
duplex {half | full}
```

```
no duplex
```

**Parameters**

- **half**—Forces half-duplex operation.
- **full**—Forces full-duplex operation.

**Default Configuration**

The interface operates in full duplex mode.
**Command Mode**

Interface Configuration (port-channel) mode

**Example**

The following example configures gi1/1/5 to operate in full duplex mode.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# duplex full
```

### 25.8 negotiation

Use the `negotiation` Interface Configuration (Ethernet, port-channel) mode command to enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface. Use the `no` form of this command to disable auto-negotiation.

**Syntax**

```
negotiation [capability [capability2 .. capability5]] [preferred {master | slave}]
no negotiation
```

**Parameters**

- **Capability**—Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f, 1000f).
  - `10h`—Advertise 10 half-duplex
  - `10f`—Advertise 10 full-duplex
  - `100h`—Advertise 100 half-duplex
  - `100f`—Advertise 100 full-duplex
  - `1000f`—Advertise 1000 full-duplex
- **Preferred**—Specifies the master-slave preference:
  - `Master`—Advertise master preference
  - `Slave`—Advertise slave preference
Default Configuration
If capability is unspecified, defaults to list of all the capabilities of the port and preferred master mode.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example enables auto-negotiation on gi1/1/5.

```
switchxxxxx(config)# interface gi1/1/5
switchxxxxx(config-if)# negotiation
```

25.9 flowcontrol
Use the `flowcontrol` Interface Configuration (Ethernet, port-channel) mode command to configure the Flow Control on a given interface. Use the `no` form of this command to disable Flow Control.

Syntax
`flowcontrol {auto / on / off}`

no flowcontrol

Parameters
- `auto`—Specifies auto-negotiation of Flow Control.
- `on`—Enables Flow Control.
- `off`—Disables Flow Control.

Default Configuration
Flow control is disabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode
User Guidelines

Use the negotiation command to enable flow control auto.

Example

The following example enables Flow Control on port gi1/1/1:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# flowcontrol on
```

25.10 mdix

Use the mdix Interface Configuration (Ethernet) mode command to enable cable crossover on a given interface. Use the no form of this command to disable cable crossover.

Syntax

```
mdix {on | auto}
no mdix
```

Parameters

- on—Enables manual MDIX.
- auto—Enables automatic MDI/MDIX.

Default Configuration

The default setting is Auto.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables automatic crossover on port gi1/1/5:

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# mdix auto
```
25.11 back-pressure

Use the `back-pressure` Interface Configuration (Ethernet) mode command to enable back pressure on a specific interface. Use the `no` form of this command to disable back pressure.

**Syntax**

- `back-pressure`
- `no back-pressure`

**Default Configuration**

Back pressure is disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

Back-pressure cannot be enabled when EEE is enabled.

**Example**

The following example enables back pressure on port gi1/1/5.

```
switchxxxxx(config)# interface gi1/1/5
switchxxxxx(config-if)# back-pressure
```

25.12 port jumbo-frame

Use the `port jumbo-frame` Global Configuration mode command to enable jumbo frames on the device. Use the `no` form of this command to disable jumbo frames.

**Syntax**

- `port jumbo-frame`
- `no port jumbo-frame`
**Default Configuration**
Jumbo frames are disabled on the device.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command takes effect only after resetting the device.

**Example**
The following example enables jumbo frames on the device.

```
switchxxxxxx(config)# port jumbo-frame
```

### 25.13 clear counters
Use the `clear counters` EXEC mode command to clear counters on all or on a specific interface.

**Syntax**

```
clear counters [interface-id]
```

**Parameters**

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

**Default Configuration**
All counters are cleared.

**Command Mode**
EXEC mode

**Example**
The following example clears the statistics counters for gi1/1/5.

```
switchxxxxxx(config)# clear counters
```
clear counters gi1/1/5.

25.14 set interface active

Use the set interface active EXEC mode command to reactivate an interface that was shut down.

Syntax

set interface active [interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

Example

The following example reactivates gi1/1/1.

set interface active gi1/1/1

25.15 errdisable recovery cause

Use the errdisable recovery cause Global Configuration mode command to enable automatic re-activation of an interface after an Err-Disable shutdown. Use the no form of this command to disable automatic re-activation.

Syntax

errdisable recovery cause {all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | udld}

no errdisable recovery cause {all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | udld}
Parameters

- **all**—Enables the error recovery mechanism for all reasons described below.
- **port-security**—Enables the error recovery mechanism for the port security Err-Disable state.
- **dot1x-src-address**—Enables the error recovery mechanism for the 802.1x Err-Disable state.
- **acl-deny**—Enables the error recovery mechanism for the ACL Deny Err-Disable state.
- **stp-bpdu-guard**—Enables the error recovery mechanism for the STP BPDU Guard Err-Disable state.
- **udld**—Enables the error recovery mechanism for the UDLD Shutdown state.

Default Configuration

Automatic re-activation is disabled.

Command Mode

Global Configuration mode

Example

The following example enables automatic re-activation of an interface after all states.

```
switchxxxxxx(config)# errdisable recovery cause all
```

25.16 **errdisable recovery interval**

Use the `errdisable recovery interval` Global Configuration mode command to set the error recovery timeout interval. Use the `no` form of this command to return to the default configuration.

Syntax

errdisable recovery interval *seconds*

no errdisable recovery interval
Parameters

**seconds**—Specifies the error recovery timeout interval in seconds. (Range: 30–86400)

Default Configuration

The default error recovery timeout interval is 300 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the error recovery timeout interval to 10 minutes.

```
switchxxxxx(config)# errdisable recovery interval 600
```

### 25.17 errdisable recovery reset

Use the `errdisable recovery reset` EXEC mode command to reactivate one or more interfaces that were shut down by a given application. A single interface, multiple interfaces or all interfaces can be specified.

Syntax

```
errdisable recovery reset {all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | udld | interface interface-id}
```

Parameters

- **all**—Reactivate all interfaces regardless of their state.
- **port-security**—Reactivate all interfaces in the Port Security Err-Disable state.
- **dot1x-src-address**—Reactivate all interfaces in the 802.1x Err-Disable state.
- **acl-deny**—Reactivate all interfaces in the ACL Deny Err-Disable state.
- **stp-bpdu-guard**—Reactivate all interfaces in the STP BPDU Guard Err-Disable state.
- **udld**—Reactivate all interfaces in the UDLD Shutdown state.
- `interface interface-id`—Reactivate interfaces that were configured to be active, but were shut down by the system.

**Default Configuration**

N/A.

**Command Mode**

EXEC mode

**Example**

**Example 1**—The following example reactivates interface gi1/1/1:

```
switchxxxxxx# errdisable recovery reset interface gi1/1/1
```

**Example 2**—The following example reactivates all interfaces regardless their state:

```
switchxxxxxx# errdisable recovery reset all
```

**Example 3**—The following example enables all interfaces in the port security Err-Disable state:

```
switchxxxxxx# errdisable recovery reset port-security
```

### 25.18 show interfaces configuration

Use the `show interfaces configuration` EXEC mode command to display the configuration for all configured interfaces or for a specific interface.

**Syntax**

```
show interfaces configuration [interface-id] [detailed]
```
Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following example displays the configuration of all configured interfaces:

```
switchxxxxxx# show interfaces configuration
```

```
Flow     Admin  Back      Mdix
Port   Type      Duplex  Speed  Neg      control  State  Pressure  Mode
------ --------- ------  -----  -------- -------  -----  --------  ----
gi1/1/1    1G-Copper Full    10000  Disabled Off      Up     Disabled  Off
        Flow  Admin

Flow      Admin
PO      Type   Speed  Neg        Control   State
------  ------ -----  --------   -------   -----             Up
Pol           Disabled   Off       Up
```

25.19  **show interfaces status**

Use the **show interfaces status** EXEC mode command to display the status of all interfaces or of a specific interface.

Syntax

```
show interfaces status [interface-id | detailed]
```

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Command Mode

EXEC mode

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Example

The following example displays the status of all configured interfaces.

```
switchxxxxxx# show interfaces status
```

```
Port  Type      Duplex Speed Neg  ctrl  State     Pressure Mode
------ --------- ------ ----- -------- ----  ------ -------- --
gi1/1/1 1G-Copper Full  1000  Disabled Off   Up     Disabled Off

Flow  Link  Back  Mdix
-----  -----  ----  ----
        Up
```

25.20  show interfaces advertise

Use the **show interfaces advertise** EXEC mode command to display auto-negotiation advertisement information for all configured interfaces or for a specific interface.

Syntax

```
show interfaces advertise [interface-id | detailed]
```
Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Examples

The following examples display auto-negotiation information.

```
switchxxxxxx# show interfaces advertise
Port Type Neg Prefere Operational Link Advertisement
---- -------- ------ ------- ---------------------------------------------
gi1/1/1 1G-Copper Enable ------- 1000f, 100f, 10f, 10h

gi1/1/2 1G-Copper Enable Master 1000f

switchxxxxxx# show interfaces advertise gi1/1/1
Port:gi1/1/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
Preference: Master
```
25.21 show interfaces description

Use the show interfaces description EXEC mode command to display the description for all configured interfaces or for a specific interface.

**Syntax**

```
show interfaces description [interface-id | detailed]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display description for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode
Example

The following example displays the description of all configured interfaces.

```
switchxxxxxx# show interfaces description
Port        Descriptions
 -----------------------------
gi1/1/1     Port that should be used for management only
...          
PO1          Output
```

25.22  show interfaces counters

Use the `show interfaces counters` EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

**Syntax**

```
show interfaces counters [interface-id | detailed]
```

**Parameters**

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `detailed`—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display counters for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode
Example

The following example displays traffic seen by all the physical interfaces.

```
switchxxxxxx# show interfaces counters gi1/1/1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
gi1/1/1           0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
gi1/1/1           0            1            35          7051
Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```
The following table describes the fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>Number of received octets.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Number of received unicast packets.</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>Number of received multicast packets.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>Number of received broadcast packets.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Number of transmitted octets.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>Number of transmitted unicast packets.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>Number of transmitted multicast packets.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Number of transmitted broadcast packets.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Number of frames received that are an integral number of octets in length but do not pass the FCS check.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>Number of frames that are involved in a single collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>Number of frames that are involved in more than one collision and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>SQE Test Errors</td>
<td>Number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.</td>
</tr>
<tr>
<td>Deferred Transmissions</td>
<td>Number of frames for which the first transmission attempt is delayed because the medium is busy.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Number of times that a collision is detected later than one slotTime into the transmission of a packet.</td>
</tr>
<tr>
<td>Excessive Collisions</td>
<td>Number of frames for which transmission fails due to excessive collisions.</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>Number of frames received that exceed the maximum permitted frame size.</td>
</tr>
<tr>
<td>Internal MAC Rx Errors</td>
<td>Number of frames for which reception fails due to an internal MAC sublayer receive error.</td>
</tr>
</tbody>
</table>
25.23 show ports jumbo-frame

Use the `show ports jumbo-frame` EXEC mode command to display whether jumbo frames are enabled on the device.

**Syntax**

```
show ports jumbo-frame
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays whether jumbo frames are enabled on the device.

```
switchxxxxxx# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```
25.24  show errdisable recovery

Use the `show errdisable recovery` EXEC mode command to display the Err-Disable configuration of the device.

**Syntax**

`show errdisable recovery`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays the Err-Disable configuration.

```
switchxxxxxx# show errdisable recovery

Timer interval: 300 Seconds

Reason     Automatic Recovery
---------------------- ------------------
port-security  Disable
dot1x-src-address  Disable
acl-deny       Enable
stp-bpdu-guard  Disable
```

25.25  show errdisable interfaces

Use the `show errdisable interfaces` EXEC mode command to display the Err-Disable state of all interfaces or of a specific interface.
### Syntax

**show errdisable interfaces** `[interface-id]`

#### Parameters

- **interface**—Interface number
- **port-channel-number**—Port channel index.

#### Default Configuration

Display for all interfaces.

#### Command Mode

EXEC mode

#### Example

The following example displays the Err-Disable state of gi1/1/50.

```
switchxxxxxx# show errdisable interfaces
Interface           Reason
------------        ------------------
  gi1/1/50                stp-bpdu-guard
```

### 25.26 storm-control broadcast enable

Use the **storm-control broadcast enable** Interface Configuration mode command to enable storm control on a port. Use the **no** form of this command to disable storm control.

#### Syntax

**storm-control broadcast enable**

**no storm-control broadcast enable**

#### Parameters

N/A
**Default Configuration**

Disabled

**Command Mode**

Interface Configuration mode (Ethernet)

**User Guidelines**

Use the `storm-control include-multicast` Interface Configuration command to count Multicast packets and optionally unknown Unicast packets in the storm control calculation.

**Example**

```
switchxxxxxxx(config)# interface gi1/1/1
switchxxxxxxx(config-if)# storm-control broadcast enable
```

### 25.27 storm-control broadcast level

Use the `storm-control broadcast level` Interface Configuration mode command to configure the maximum rate of broadcast. Use the `no` form of this command to return to default.

**Syntax**

```
storm-control broadcast level {level | kbps kbps}
no storm-control broadcast level
```

**Parameters**

- **level**—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1-100)

- **kbps**—Maximum of kilobits per second of broadcast traffic on a port. (Range 70 –10000000)

**Default Configuration**

10% of port speed in Kbps
**Command Mode**

Interface Configuration mode (Ethernet)

**User Guidelines**

Use the `storm-control broadcast enable` Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

**Example**

**Example 1**—Set to specific level:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# storm-control broadcast level 20
```

**Example 2**—set to specific rate:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# storm-control broadcast kbps 10000
```

25.28  **storm-control include-multicast**

Use the `storm-control include-multicast` Interface Configuration mode command to count Multicast packets in a Broadcast storm control. Use the `no` form of this command to disable counting of Multicast packets in the Broadcast storm control.

**Syntax**

```
storm-control include-multicast [unknown-unicast]
no storm-control include-multicast
```

**Parameters**

- `unknown-unicast`—Specifies also the count of unknown unicast packets.

**Default Configuration**

Disabled
**Command Mode**

Interface Configuration mode (Ethernet)

**Example**

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# storm-control include-multicast
```

**25.29 show storm-control**

Use the `show storm-control` EXEC mode command to display the configuration of storm control for a port.

**Syntax**

```
show storm-control [interface-id]
```

**Parameters**

- `interface-id`—Specifies the Ethernet port.

**Default Configuration**

Display for all interfaces.

**Command Mode**

EXEC mode

**Example**

```
switchxxxxxx# show storm-control
```

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Admin Rate</th>
<th>Oper Rate</th>
<th>Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1</td>
<td>Enabled</td>
<td>12345 Kb/Sec</td>
<td>12345 Kb/Sec</td>
<td>Broadcast, Multicast, Unknown Unicast</td>
</tr>
<tr>
<td>gi1/2</td>
<td>Disabled</td>
<td>100000 Kb/Sec</td>
<td>100000 Kb/Sec</td>
<td>Broadcast</td>
</tr>
<tr>
<td>gi1/3</td>
<td>Enabled</td>
<td>10%</td>
<td>000000000000</td>
<td>Broadcast</td>
</tr>
</tbody>
</table>
PHY Diagnostics Commands

26.1 test cable-diagnostics tdr

Use the test cable-diagnostics tdr Privileged EXEC mode command to use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test cable-diagnostics tdr interface interface-id

Parameters

interface-id—Specifies an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

This command does not work on fiber ports (if they exist on the device). The port to be tested should be shut down during the test, unless it is a combination port with fiber port active. In this case, it does not need to be shut down, because the test does not work on fiber ports.

The maximum length of cable for the TDR test is 120 meters.

Example

Example 1 - Test the copper cables attached to port 1 (a copper port).

switchxxxxxx# test cable-diagnostics tdr interface gi1/1/1
Cable is open at 64 meters

Example 2 - Test the copper cables attached to port 2 (a combo port with fiber active).

switchxxxxxx# test cable-diagnostics tdr interface gi1/1/2
Fiber ports are not supported

26.2 show cable-diagnostics tdr

Use the `show cable-diagnostics tdr` EXEC mode command to display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port.

Syntax

`show cable-diagnostics tdr [interface interface-id | detailed]`

Parameters

- `interface-id`—Specify an Ethernet port ID.
- `detailed`—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
switchxxxxxx# show cable-diagnostics tdr
Port       Result    Length [meters]   Date          
--------    --------   -----------   --------------
          OK            
          Short       50  13:32:00  23 July 2010
        Test has not been performed
          Open        64  13:32:00  23 July 2010
```
26.3  show cable-diagnostics cable-length

Use the show cable-diagnostics cable-length EXEC mode command to display the estimated copper cable length attached to all ports or to a specific port.

Syntax

show cable-diagnostics cable-length [interface interface-id | detailed]

Parameters

- interface-id—Specify an Ethernet port ID.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

User Guidelines

The port must be active and working at 100 M or 1000 M.

Example

The following example displays the estimated copper cable length attached to all ports.

```
switchxxxxxx# show cable-diagnostics cable-length
Port    Length [meters]
---      ----------------
gi1/1/1  < 50
Copper not active
gi1/1/3  110-140
```
26.4 show fiber-ports optical-transceiver

Use the show fiber-ports optical-transceiver EXEC mode command to display the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [interface interface-id | detailed]

Parameters

- interface-id—Specify an Ethernet port ID.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following examples display the optical transceiver diagnostics results.

```
switchxxxxxx# show fiber-ports optical-transceiver
Port      Temp  Voltage Current  Output Input   LOS
          Power  Power
----------- ------ ------- -------  ------ -----   ---
  gi1/1/1       W       OK      OK     OK     OK      OK
  gi1/1/2       OK      OK      OK     E      OK      OK
Temp         - Internally measured transceiver temperature
Voltage      - Internally measured supply voltage
Current      - Measured TX bias current
Output Power - Measured TX output power in milliWatts
Input Power  - Measured RX received power in milliWatts
LOS          - Loss of signal
```
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error

```
switchxxxxxx# show fiber-ports optical-transceiver

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output Power</th>
<th>Input Power</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>28</td>
<td>3.32</td>
<td>7.26</td>
<td>3.53</td>
<td>3.68</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/6</td>
<td>29</td>
<td>3.33</td>
<td>6.50</td>
<td>3.53</td>
<td>3.71</td>
<td>No</td>
</tr>
</tbody>
</table>

- Temp: Internally measured transceiver temperature
- Voltage: Internally measured supply voltage
- Current: Measured TX bias current
- Output Power: Measured TX output power in milliWatts
- Input Power: Measured RX received power in milliWatts
- LOS: Loss of signal

N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```
27.1 power inline

Use the power inline Interface Configuration mode command to configure the inline power administrative mode on an interface.

Syntax

```
power inline auto [time-range time-range-name]
power inline never
```

Parameters

- **auto**—Turns on the device discovery protocol and applies power to the device.
- **never**—Turns off the device discovery protocol and stops supplying power to the device.
- **time-range-name**—Specifies a time range. When the time range is not in effect the power is not supplied to the attached device. If a time range is not specified, there is no time range bounded to the port. (Range: 1–32 characters)

Default Configuration

The default configuration is set to auto.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The **never** parameter cannot be used with a time range.

Example

The following example turns on the device discovery protocol on port 4.

```
switchxxxxxx(config)# interface gi1/1/4
```
27 Power over Ethernet (PoE) Commands

27.2 power inline inrush test disable

Use the **power inline inrush test disable** Global Configuration mode command to disable the inrush test (a hardware test that checks input surge current for PoE devices). Use the no form of this command to enable the inrush test.

**Syntax**

```plaintext
power inline inrush test disable
no power inline inrush test disable
```

**Parameters**

N/A.

**Default Configuration**

Inrush test is enabled.

**Command Mode**

Global Configuration mode

**Example**

The following example disables inrush test.

```
switchxxxxxx(config)# power inline inrush test disable
```

27.3 power inline legacy support disable

Use the **power inline legacy support disable** Global Configuration mode command to disable the legacy PDs support. Use the no form of this command to enable the legacy support.

**Syntax**

```plaintext
power inline legacy support disable
no power inline legacy support disable
```

**Parameters**

N/A.
Default Configuration
Legacy support is enabled.

Command Mode
Global Configuration mode

Example
The following example disables legacy PDs support.

```
switchxxxxxx(config)# power legacy support disable
```

### 27.4 power inline powered-device

Use the `power inline powered-device` Interface Configuration mode command to add a description of the powered device type. Use the `no` form of this command to remove the description.

**Syntax**

```
power inline powered-device pd-type
no power inline powered-device
```

**Parameters**

`pd-type`—Enters a comment or a description to assist in recognizing the type of the powered device attached to this interface. (Length: 1–24 characters)

**Default Configuration**

There is no description.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example adds the description ‘ip phone’ of the device connected to port 4.

```
switchxxxxxx(config)# interface gi1/1/4
switchxxxxxx(config-if)# power inline powered-device ip_phone
```
27.5 **power inline priority**

Use the `power inline priority` Interface Configuration (Ethernet) mode command to configure the interface inline power management priority. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
power inline priority {critical | high | low}
no power inline priority
```

**Parameters**

- **critical**—Specifies that the powered device operation is critical.
- **high**—Specifies that the powered device operation is high priority.
- **low**—Specifies that the powered device operation is low priority.

**Default Configuration**

The default configuration is set to low priority.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example sets the inline power management priority of port gi1/1/4 to High.

```
switchxxxxxx(config)# interface gi1/1/4
switchxxxxxx(config-if)# power inline priority high
```

27.6 **power inline usage-threshold**

Use the `power inline usage-threshold` Global Configuration mode command to configure the threshold for initiating inline power usage alarms. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
power inline usage-threshold percent
```

**Example**

```
switchxxxxxx(config)# power inline usage-threshold 70
```
no power inline usage-threshold

Parameters

percent—Specifies the threshold in percent to compare to the measured power. (Range: 1–99)

Default Configuration

The default threshold is 95 percent.

Command Mode

Global Configuration mode

Example

The following example configures the threshold for initiating inline power usage alarms to 90 percent.

switchxxxxxx(config)# power inline usage-threshold 90

27.7 power inline traps enable

Use the power inline traps enable Global Configuration mode command to enable inline power traps. Use the no form of this command to disable traps.

Syntax

power inline traps enable
no power inline traps enable

Default Configuration

Inline power traps are disabled.

Command Mode

Global Configuration mode

Example

The following example enables inline power traps.
switchxxxxxx(config)# power inline traps enable

27.8 power inline limit

Use the `power inline limit` Interface Configuration mode command to configure the power limit per port on an interface. Use the `no` form of the command to return to default.

Syntax

```
power inline limit power
no power inline limit
```

Parameters

- `power`—States the port power consumption limit in Milliwatts (Range: 0-154000–30000)

Default Configuration

The default value is the maximum power allowed in the specific working mode: 15.4W 30W

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The operational power limit is the minimum of the configured power limit value and the maximum power capability on port. For example, if the configured value is higher than 15.4W on a PoE port, the operational power limit is 15.4W.

Example

The following example sets inline power on a port.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# power inline limit 2222
```
27.9  power inline limit-mode

Use the power inline limit-mode Global Configuration mode command to set the power limit mode of the system. Use the no form of this command to return to default.

Syntax

```
power inline limit-mode {class | port}
```

Examples

```
no power inline limit-mode
```

Parameters

- **class**—The power limit of a port is based on the class of the PD (Power Device) as detected during the classification process.
- **port**—The power limit of a port is fixed regardless of the class of the discovered PD.

Command Mode

Global Configuration mode

User Guidelines

Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE ports.

Example

The following example sets the power limit to class.

```
switchxxxxxx(config)# power inline limit-mode class

"Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE ports. Are you sure? [y/n]"
```

27.10  show power inline

Use the show power inline EXEC mode command to display information about the inline power for all interfaces or for a specific interface.
Syntax

show power inline [interface-id | detailed \ module unit-id]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- **module unit-id**—Specifies the unit ID of the stack member.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Show information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

User Guidelines

Sometimes when a port requests more power that its limit, it may show that the port gets power even though no power is supplied to the port.

Example

The following example displays information about the inline power for all ports (port power based).

switchxxxxxx(config)# show power inline
Power limit: 15 W
Power limit (for port based power-limit mode): 15 W

<table>
<thead>
<tr>
<th>Unit</th>
<th>Power</th>
<th>Nominal Power</th>
<th>Consumed</th>
<th>Usage</th>
<th>Traps</th>
<th>Inrush Test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off</td>
<td>1 Watts</td>
<td>0 Watts (0%)</td>
<td>95</td>
<td>Disable</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
## Power over Ethernet (PoE) Commands

<table>
<thead>
<tr>
<th>Port</th>
<th>Powered Device</th>
<th>State</th>
<th>Status</th>
<th>Priority</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>IP Phone Model A</td>
<td>Auto</td>
<td>On</td>
<td>High</td>
<td>Class0</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Wireless AP Model A</td>
<td>Auto</td>
<td>On</td>
<td>Low</td>
<td>Class1</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td></td>
<td>Auto</td>
<td>Off</td>
<td>Low</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Example

The following example displays information about the inline power for a specific port.

```
switchxxxxxx(config)# show power inline gi1/1/1
```

Power limit: 15 W
Power limit (for port based power-limit mode): 15 W

<table>
<thead>
<tr>
<th>Port</th>
<th>Powered Device</th>
<th>State</th>
<th>Status</th>
<th>Priority</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>IP Phone Model A</td>
<td>Auto</td>
<td>On</td>
<td>High</td>
<td>Class0</td>
</tr>
</tbody>
</table>

Time range:

Power limit: 30.0 W
Overload Counter: 0
Short Counter: 0
Denied Counter: 0
Absent Counter: 0
Invalid Signature Counter: 0
The following table describes the fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Inline power sourcing equipment operational status.</td>
</tr>
<tr>
<td>Nominal Power</td>
<td>Inline power sourcing equipment nominal power in Watts.</td>
</tr>
<tr>
<td>Consumed Power</td>
<td>Measured usage power in Watts.</td>
</tr>
<tr>
<td>Usage Threshold</td>
<td>Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.</td>
</tr>
<tr>
<td>Traps</td>
<td>Indicates if inline power traps are enabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Ethernet port number.</td>
</tr>
<tr>
<td>Powered device</td>
<td>Description of the powered device type.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates if the port is enabled to provide power. The possible values are Auto or Never.</td>
</tr>
<tr>
<td>Priority</td>
<td>Port inline power management priority. The possible values are Critical, High or Low.</td>
</tr>
<tr>
<td>Status</td>
<td>Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.</td>
</tr>
<tr>
<td>Class</td>
<td>Power consumption classification of the powered device.</td>
</tr>
<tr>
<td>Overload Counter</td>
<td>Counts the number of overload conditions detected.</td>
</tr>
<tr>
<td>Short Counter</td>
<td>Counts the number of short conditions detected.</td>
</tr>
<tr>
<td>Denied Counter</td>
<td>Counts the number of times power was denied.</td>
</tr>
<tr>
<td>Absent Counter</td>
<td>Counts the number of times power was removed because powered device dropout was detected.</td>
</tr>
<tr>
<td>Invalid Signature Counter</td>
<td>Counts the number of times an invalid signature of a powered device was detected.</td>
</tr>
<tr>
<td>Inrush Test</td>
<td>Displays whether the inrush test is enabled or disabled.</td>
</tr>
</tbody>
</table>

Following is a list of port status values:

Port is off - Underload disconnect detected

Port is off - Overload detected

Port is off - Short detected
Port is off - Invalid PD resistor signature detected
Port is on - Valid PD resistor signature detected
Port is off - Power was denied
Port is on - Valid capacitor signature detected
Port is off - Backoff state has occurred
Port is off - Class error has occurred

27.11 show power inline consumption

Use the show power inline consumption EXEC mode command to display information about the inline power consumption for all interfaces or for a specific interface.

Syntax

show power inline consumption [interface-id | detailed | module stack-member-number]

Parameters

- **Interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- **module stack-member-number**—Specifies the switch member in a stack.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Show information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode
**Example**

The following example displays information about the inline power consumption.

```
switchxxxxxx# show power inline consumption
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Power Limit (W)</th>
<th>Power (W)</th>
<th>Voltage (V)</th>
<th>Current (mA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>15.4</td>
<td>4.115</td>
<td>50.8</td>
<td>81</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>15.4</td>
<td>4.157</td>
<td>50.7</td>
<td>82</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>30</td>
<td>15.4</td>
<td>50.9</td>
<td>79</td>
</tr>
</tbody>
</table>
28.1 eee enable (global)

Use the `eee enable` Global Configuration command to enable the EEE mode globally. Use the `no` format of the command to disable the mode.

**Syntax**

```
eee enable
no eee enable
```

**Default Configuration**

EEE is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

In order for EEE to work, the device at the other end of the link must also support EEE and have it enabled. In addition, for EEE to work properly, auto-negotiation must be enabled; however, if the port speed is negotiated as 1Giga, EEE always works regardless of whether the auto-negotiation status is enabled or disabled.

If auto-negotiation is not enabled on the port and its speed is less than 1 Giga, the EEE operational status is disabled.

**Example**

```
switchxxxxxx(conf)# eee enable
```

28.2 eee enable (interface)

Use the `eee enable` Interface Configuration command to enable the EEE mode on an Ethernet port. Use the `no` format of the command to disable the mode.
**Syntax**

`eee enable`

`no eee enable`

**Parameters**

N/A

**Default Configuration**

EEE is enabled.

**Command Mode**

Interface Configuration mode (Ethernet)

**User Guidelines**

If auto-negotiation is not enabled on the port and its speed is 1 Giga, the EEE operational status is disabled.

**Example**

```
switchxxxxxx(conf)#interface gi1/1/1
switchxxxxxx(conf-if)#eee enable
```

### 28.3 eee lldp enable

Use the `eee lldp enable` Interface Configuration command to enable EEE support by LLDP on an Ethernet port. Use the `no` format of the command to disable the support.

**Syntax**

`eee lldp enable`

`no eee lldp enable`

**Parameters**

N/A
Default Configuration
Enabled

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Enabling EEE LLDP advertisement enables devices to choose and change system wake-up times in order to get the optimal energy saving mode.

Example

switchxxxxxx(conf)#interface gi1/1/1
switchxxxxxx(conf-if)#eee lldp enable

28.4 show eee
Use the show eee EXEC command to display EEE information.

Syntax
show eee [interface-id]

Parameters
interface-id—Specify an Ethernet port.

Defaults
N/A

Command Mode
EXEC

Examples

Example 1 - The following displays brief Information about all ports.

switchxxxxxx#show eee
EEE globally enabled

EEE Administrate status is enabled on ports: gi1/1/1-6, gi1/1/7
EEE Operational status is enabled on ports: gi1/1/1, gi1/1/3-6, gi1/1/2, gi1/1/5
EEE LLDP Administrate status is enabled on ports: gi1/1/1-5
EEE LLDP Operational status is enabled on ports: gi1/1/1-5

Example 2 - The following is the information displayed when a port is in the Not Present state; no information is displayed if the port supports EEE.

```
switchxxxxxx# show eee gi1/1/10
Port Status: notPresent
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 3 - The following is the information displayed when the port is in status DOWN.

```
switchxxxxxx# show eee gi1/1/10
Port Status: DOWN
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  EEE Administrate status: enabled
  EEE LLDP Administrate status: enabled
```

Example 4 - The following is the information displayed when the port is in status UP and does not support EEE.

```
switchxxxxxx# show eee gi1/1/2
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
```
EEE Commands

Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled

**Example 5** - The following is the information displayed when the neighbor does not support EEE.

```
switchxxxxxx#show eee gi1/1/5
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

**Example 6** - The following is the information displayed when EEE is disabled on the port.

```
switchxxxxxx#show eee gi1/1/1
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: enabled
```
EEE Operational status: disabled

**Example 7** - The following is the information displayed when EEE is running on the port, and EEE LLDP is disabled.

```
switchxxxxxx# show eee gi1/1/2
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
```

**Example 8** - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
switchxxxxxx# show eee gi1/1/3
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
```
EEE Operational status: enabled
EEE LLDP Administrative status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec

Example 9 - The following is the information displayed when EEE is running on the port, EEE LLDP is enabled but not synchronized with the remote link partner.

switchxxxxxx#show eee gi1/1/9
Port Status: up
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrative status: enabled
EEE Operational status: enabled
EEE LLDP Administrative status: enabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
Example 10 - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
switchxxxxxx#show eee gi1/1/3
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```
Green Ethernet

29.1 green-ethernet energy-detect (global)

Use the green-ethernet energy-detect Global Configuration mode command to enable Green-Ethernet Energy-Detect mode globally. Use the no form of this command to disabled it.

Syntax

green-ethernet energy-detect

no green-ethernet energy-detect

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

switchxxxxxx(config)# green-ethernet energy-detect

29.2 green-ethernet energy-detect (interface)

Use the green-ethernet energy-detect Interface configuration mode command to enable green-ethernet Energy-Detect mode on a port. Use the no form of this command, to disable it on a port.

Syntax

green-ethernet energy-detect

no green-ethernet energy-detect
Parameters
N/A

Default Configuration
Disabled

Command Mode
Interface configuration mode (Ethernet)

User Guidelines
Energy-Detect can work only when the port is a copper port. When a port is enabled for auto selection, copper/fiber Energy-Detect cannot work.

It takes the PHY ~5 seconds to fall into sleep mode when the link is lost after normal operation.

Example

```
switchxxxxx(config)# interface gi1/1/1
switchxxxxx(config-if)# green-ethernet energy-detect
```

29.3  green-ethernet short-reach (global)

Use the `green-ethernet short-reach` Global Configuration mode command to enable green-ethernet short-reach mode globally. Use the `no` form of this command to disabled it.

Syntax

green-ethernet short-reach

no green-ethernet short-reach

Parameters

N/A

Default Configuration

Disabled.
Command Mode
Global Configuration mode

Example

switchxxxxxx(config)# green-ethernet short-reach

29.4 green-ethernet short-reach (interface)
Use the `green-ethernet short-reach` Interface Configuration mode command to enable green-ethernet short-reach mode on a port. Use the `no` form of this command to disable it on a port.

Syntax

`green-ethernet short-reach`
`no green-ethernet short-reach`

Parameters

N/A

Default Configuration

Disabled.

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines

When **Short-Reach** mode is enabled and is not forced, the VCT (Virtual Cable Tester) length check must be performed. The VCT length check can be performed only on a copper port operating at a speed of 1000 Mbps. If the media is not copper or the link speed is not 1000 Mbps, Short-Reach mode is not applied.

When the interface is set to enhanced mode, after the VCT length check has completed and set the power to low, an active monitoring for errors is done continuously. In the case of errors crossing a certain threshold, the PHY will be reverted to long reach.

Note that EEE cannot be enabled if the Short-Reach mode is enabled.
Example

switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# green-ethernet short-reach

29.5 green-ethernet power-meter reset

Use the green-ethernet power-meter reset Privileged EXEC mode command to reset the power save meter.

Syntax

green-ethernet power-meter reset

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode.

Example

switchxxxxxx# green-ethernet power-meter reset

29.6 show green-ethernet

Use the show green-ethernet Privileged EXEC mode command to display green-ethernet configuration and information.

Syntax

show green-ethernet [interface-id | detailed]

Parameters

- interface-id—Specifies an Ethernet port
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display for all ports. If detailed is not used, only present ports are displayed.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

The power savings displayed is relevant to the power saved by short reach, energy detect and disable port LEDs.

The EEE power saving is dynamic by nature since it is based on port utilization and is therefore not taken into consideration.

The following describes the reasons for non-operation displayed by this command.

If there are a several reasons, then only the highest priority reason is displayed.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NP</td>
<td>Port is not present</td>
</tr>
<tr>
<td>2</td>
<td>LT</td>
<td>Link Type is not supported (fiber, auto media select)</td>
</tr>
<tr>
<td>3</td>
<td>LU</td>
<td>Port Link is up – NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Priority</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NP</td>
<td>Port is not present</td>
</tr>
<tr>
<td>2</td>
<td>LT</td>
<td>Link Type is not supported (fiber)</td>
</tr>
<tr>
<td>3</td>
<td>LS</td>
<td>Link Speed Is not Supported (100M, 10M, 10G)</td>
</tr>
<tr>
<td>4</td>
<td>LL</td>
<td>Link Length received from VCT test exceeds threshold</td>
</tr>
<tr>
<td>6</td>
<td>LD</td>
<td>Port Link is Down – NA</td>
</tr>
</tbody>
</table>
**Example**

```
switchxxxxxx# show green-ethernet

Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Disable Port LEDs mode: Enabled
Power Savings: 24% (1.08W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
Short-Reach cable length threshold: 50m

<table>
<thead>
<tr>
<th>Port</th>
<th>Energy-Detect</th>
<th>Short-Reach</th>
<th>VCT Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Admin Oper Reason</td>
<td>Admin Force Oper Reason</td>
<td>Length</td>
</tr>
<tr>
<td></td>
<td>-----</td>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>gi1/1/1</td>
<td>on</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>on</td>
<td>off</td>
<td>LU</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>on</td>
<td>off</td>
<td>LU</td>
</tr>
</tbody>
</table>
```
Port Channel Commands

30.1 channel-group

Use the *channel-group* Interface Configuration (Ethernet) mode command to associate a port with a port-channel. Use the *no* form of this command to remove a port from a port-channel.

**Syntax**

```
channel-group port-channel mode {on | auto}

no channel-group
```

**Parameters**

- **port-channel**—Specifies the port channel number for the current port to join.
- **mode**—Specifies the mode of joining the port channel. The possible values are:
  - **on**—Forces the port to join a channel without an LACP operation.
  - **auto**—Forces the port to join a channel as a result of an LACP operation.

**Default Configuration**

The port is not assigned to a port-channel.

**Command Mode**

Interface Configuration (Ethernet) mode

**Default mode is on.**

**Example**

The following example forces port gi1/1/1 to join port-channel 1 without an LACP operation.

```
switchxxxxxxx(config)# interface gi1/1/1
switchxxxxxxx(config-if)# channel-group 1 mode on
```
30.2  port-channel load-balance

Use the **port-channel load-balance** Global Configuration mode command to configure the load balancing policy of the port channeling. Use the **no** form of this command to reset to default.

**Syntax**

```
port-channel load-balance {src-dst-mac| src-dst-mac-ip}
```

**Parameters**

- **src-dst-mac**—Port channel load balancing is based on the source and destination MAC addresses.
- **src-dst-mac-ip**—Port channel load balancing is based on the source and destination of MAC and IP addresses.

**Default Configuration**

src-dst-mac is the default option.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxxx(config)# port-channel load-balance src-dst-mac
switchxxxxxxx(config)# port-channel load-balance src-dst-mac-ip
```

30.3  show interfaces port-channel

Use the **show interfaces port-channel** EXEC mode command to display port-channel information for all port channels or for a specific port channel.

**Syntax**

```
show interfaces port-channel [interface-id]
```
Parameters
interface-id—Specify an interface ID. The interface ID must be a Port Channel.

Command Mode
EXEC mode

Examples
The following example displays information on all port-channels.

```
switchxxxxxx# show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel  Ports
-------  ----- 
P01   Active: gi1/1, Inactive: gi1/1/2-3
P02   Active: gi1/1/5, Inactive: gi1/1/4
```
31.1 bridge multicast filtering

Use the \texttt{bridge multicast filtering} Global Configuration mode command to enable the filtering of Multicast addresses. Use the \texttt{no} form of this command to disable Multicast address filtering.

\textbf{Syntax}

\begin{verbatim}
bridge multicast filtering
no bridge multicast filtering
\end{verbatim}

\textbf{Default Configuration}

Multicast address filtering is disabled. All Multicast addresses are flooded to all ports.

\textbf{Command Mode}

Global Configuration mode

\textbf{User Guidelines}

When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

All registered Multicast addresses will be forwarded to the Multicast groups. There are two ways to manage Multicast groups, one is the IGMP Snooping feature, and the other is the \texttt{bridge multicast forward-all} command.

\textbf{Example}

The following example enables bridge Multicast filtering.

\begin{verbatim}
switchxxxxxx(config)# bridge multicast filtering
\end{verbatim}
31.2 bridge multicast mode

Use the bridge multicast mode Interface Configuration (VLAN) mode command to configure the Multicast bridging mode. Use the no form of this command to return to the default configuration.

Syntax

bridge multicast mode {mac-group /ipv4-group /ipv4-src-group}

no bridge multicast mode

Parameters

- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address.
- **ipv4-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.
- **ipv4-src-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

Default Configuration

The default mode is mac-group.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the mac-group option when using a network management system that uses a MIB based on the Multicast MAC address. Otherwise, it is recommended to use the ipv4-group or ipv4-src-group mode, because there is no overlapping of IPv4 Multicast addresses in these modes.
For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

<table>
<thead>
<tr>
<th>FDB Mode</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>bridge multicast address</td>
</tr>
<tr>
<td></td>
<td>bridge multicast forbidden address</td>
</tr>
<tr>
<td>ipv4-group</td>
<td>bridge multicast ip-address</td>
</tr>
<tr>
<td></td>
<td>bridge multicast forbidden ip-address</td>
</tr>
<tr>
<td>ipv4-src-group</td>
<td>bridge multicast source group</td>
</tr>
<tr>
<td></td>
<td>bridge multicast forbidden source group</td>
</tr>
</tbody>
</table>

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

<table>
<thead>
<tr>
<th>FDB mode</th>
<th>IGMP version 2</th>
<th>IGMP version 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>MAC group address</td>
<td>MAC group address</td>
</tr>
<tr>
<td>ipv4-group</td>
<td>IP group address</td>
<td>IP group address</td>
</tr>
<tr>
<td>ipv4-src-group</td>
<td>(*)</td>
<td>IP source and group addresses</td>
</tr>
</tbody>
</table>

(*) Note that (*,G) cannot be written to the FDB if the mode is ipv4-src-group. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (*,G), the operating FDB mode is changed to ipv4-group.

**Example**

The following example configures the Multicast bridging mode as an ipv4-group on VLAN 2.

```plaintext
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast mode ipv4-group
```

### 31.3 bridge multicast address

Use the **bridge multicast address** Interface Configuration (VLAN) mode command to register a MAC-layer Multicast address in the bridge table and statically add or
remove ports to or from the group. Use the no form of this command to unregister the MAC address.

Syntax

bridge multicast address {mac-multicast-address | ipv4-multicast-address} [add | remove] [ethernet interface-list | port-channel port-channel-list]

no bridge multicast address {mac-multicast-address}

Parameters

- mac-multicast-address | ipv4-multicast-address—Specifies the group Multicast address.
- add—Adds ports to the group.
- remove—Removes ports from the group.
- ethernet interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

If ethernet interface-list or port-channel port-channel-list is specified without specifying add or remove, the default option is add.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the mac-multicast-address parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.
Examples

Example 1 - The following example registers the MAC address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03
```

Example 2 - The following example registers the MAC address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03 add gi1/1/1-2
```

31.4 bridge multicast forbidden address

Use the `bridge multicast forbidden address` Interface Configuration (VLAN) mode command to forbid adding or removing a specific Multicast address to or from specific ports. Use the `no` form of this command to restore the default configuration.

Syntax

```
bridge multicast forbidden address {mac-multicast-address | ipv4-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}

no bridge multicast forbidden address {mac-multicast-address}
```

Parameters

- **mac-multicast-address | ipv4-multicast-address**—Specifies the group Multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**

No forbidden addresses are defined.

Default option is **add**.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Before defining forbidden ports, the Multicast group should be registered, using **bridge multicast address**.

You can execute the command before the VLAN is created.

**Example**

The following example forbids MAC address 0100.5e02.0203 on port gi1/1/9 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 0100.5e02.0203
switchxxxxxx(config-if)# bridge multicast forbidden address 0100.5e02.0203
   add gi1/1/9
```

### 31.5 bridge multicast ip-address

Use the **bridge multicast ip-address** Interface Configuration (VLAN) mode command to register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group. Use the no form of this command to unregister the IP address.

**Syntax**

```
bridge multicast ip-address ip-multicast-address [add | remove] [interface-list | port-channel port-channel-list]
```

```
no bridge multicast ip-address ip-multicast-address
```
Parameters

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

Default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **ip-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

The following example registers the specified IP address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
```

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

```
switchxxxxxx(config)# interface vlan 8
```
31.6 bridge multicast forbidden ip-address

Use the bridge multicast forbidden ip-address Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP Multicast address to or from specific ports. Use the no form of this command to restore the default configuration.

Syntax

```bash
bridge multicast forbidden ip-address {ip-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}
no bridge multicast forbidden ip-address {ip-multicast-address}
```

Parameters

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.
You can execute the command before the VLAN is created.
Example

The following example registers IP address 239.2.2.2, and forbids the IP address on port gi1/1/9 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden ip-address 239.2.2.2 add gi1/1/9
```

31.7 bridge multicast source group

Use the **bridge multicast source group** Interface Configuration (VLAN) mode command to register a source IP address - Multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the no form of this command to unregister the source-group-pair.

**Syntax**

```
bridge multicast source ip-address group ip-multicast-address [[add | remove] [ethernet interface-list | port-channel port-channel-list]]
no bridge multicast source ip-address group ip-multicast-address
```

**Parameters**

- **ip-address**—Specifies the source IP address.
- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group for the specific source IP address.
- **remove**—Removes ports from the group for the specific source IP address.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

No Multicast addresses are defined.
The default option is **add**.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

The following example registers a source IP address - Multicast IP address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
```

### 31.8 bridge multicast forbidden source group

Use the **bridge multicast forbidden source group** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports. Use the no form of this command to return to the default configuration.

**Syntax**

```
bridge multicast forbidden source ip-address group ip-multicast-address [add |
remove] [ethernet interface-list | port-channel port-channel-list]
no bridge multicast forbidden source ip-address group ip-multicast-address
```

**Parameters**

- **ip-address**—Specifies the source IP address.
- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Forbids adding ports to the group for the specific source IP address.
- **remove**—Forbids removing ports from the group for the specific source IP address.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

No forbidden addresses are defined.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

**Example**

The following example registers a source IP address - Multicast IP address pair to the bridge table, and forbids adding the pair to port gi1/1/9 on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden source 13.16.1.1 group 239.2.2.2 add gi1/1/9
```

**31.9 bridge multicast ipv6 mode**

Use the **bridge multicast ipv6 mode** Interface Configuration (VLAN) mode command to configure the Multicast bridging mode for IPv6 Multicast packets. Use the no form of this command to return to the default configuration.

**Syntax**

```
bridge multicast ipv6 mode {mac-group / ip-group / ip-src-group}
no bridge multicast ipv6 mode
```
Parameters

- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC destination address.
- **ip-group**—Specifies that Multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- **ip-src-group**—Specifies that Multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

Default Configuration

The default mode is **mac-group**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **mac-group** mode when using a network management system that uses a MIB based on the Multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 Multicast addresses in the FDB, as described in the following table:

<table>
<thead>
<tr>
<th>FDB Mode</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>bridge multicast address</td>
</tr>
<tr>
<td>ipv6-group</td>
<td>bridge multicast ipv6 ip-address</td>
</tr>
<tr>
<td>ipv6-src-group</td>
<td>bridge multicast ipv6 source group</td>
</tr>
</tbody>
</table>

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network: (*

<table>
<thead>
<tr>
<th>FDB mode</th>
<th>MLD version 1</th>
<th>MLD version 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>MAC group address</td>
<td>MAC group address</td>
</tr>
<tr>
<td>ipv6-group</td>
<td>IPv6 group address</td>
<td>IPv6 group address</td>
</tr>
<tr>
<td>ipv6-src-group</td>
<td>(*)</td>
<td>IPv6 source and group addresses</td>
</tr>
</tbody>
</table>
Note that (*,G) cannot be written to the FDB if the mode is **ip-src-group**. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group. If an application on the device requests (*,G), the operating FDB mode is changed to **ip-group**.

You can execute the command before the VLAN is created.

**Example**

The following example configures the Multicast bridging mode as an **ip-group** on VLAN 2.

```bash
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast ipv6 mode ip-group
```

### 31.10 bridge multicast ipv6 ip-address

Use the **bridge multicast ipv6 ip-address** Interface Configuration (VLAN) mode command to register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the IPv6 address.

**Syntax**

```
bridge multicast ipv6 ip-address ipv6-multicast-address [[add | remove] [ethernet interface-list / port-channel port-channel-list]]
```

**Parameters**

- **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.
Default Configuration
No Multicast addresses are defined.
The default option is add.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
To register the group in the bridge database without adding or removing ports or port channels, specify the `ipv6-multicast-address` parameter only.

Static Multicast addresses can be defined on static VLANs only.
You can execute the command before the VLAN is created.

Example
Example 1 - The following example registers the IPv6 address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:4:4:4:1
```

Example 2 - The following example registers the IPv6 address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:4:4:4:1 add gi1/1/1-2
```

31.11 bridge multicast ipv6 forbidden ip-address
Use the `bridge multicast ipv6 forbidden ip-address` Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 Multicast address to or from specific ports. To restore the default configuration, use the `no` form of this command.
Syntax

bridge multicast ipv6 forbidden ip-address \{ipv6-multicast-address\} \{add | remove\} \{ethernet interface-list | port-channel port-channel-list\}

no bridge multicast ipv6 forbidden ip-address \{ipv6-multicast-address\}

Parameters

- ipv6-multicast-address—Specifies the group IPv6 Multicast address.
- add—Forbids adding ports to the group.
- remove—Forbids removing ports from the group.
- ethernet interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

The default option is add.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers an IPv6 Multicast address, and forbids the IPv6 address on port gi1/1/9 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```
switchxxxxx(config-if)# bridge multicast ipv6 forbidden ip-address
FF00::0:0:4:4:4:1 add gi1/1/9

### 31.12 bridge multicast ipv6 source group

Use the `bridge multicast ipv6 source group` Interface Configuration (VLAN) mode command to register a source IPv6 address - Multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the `no` form of this command to unregister the source-group-pair.

**Syntax**

```
bridge multicast ipv6 source ipv6-source-address group ipv6-multicast-address
   [[add | remove] {ethernet interface-list | port-channel port-channel-list}]
no bridge multicast ipv6 source ipv6-address group ipv6-multicast-address
```

**Parameters**

- `ipv6-source-address`—Specifies the source IPv6 address.
- `ipv6-multicast-address`—Specifies the group IPv6 Multicast address.
- `add`—Adds ports to the group for the specific source IPv6 address.
- `remove`—Removes ports from the group for the specific source IPv6 address.
- `ethernet interface-list`—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**

No Multicast addresses are defined.

The default option is `add`.

**Command Mode**

Interface Configuration (VLAN) mode
Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8

switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
```

31.13 bridge multicast ipv6 forbidden source group

Use the `bridge multicast ipv6 forbidden source group` Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports. Use the no form of this command to return to the default configuration.

Syntax

```
bridge multicast ipv6 forbidden source ipv6-source-address group ipv6-multicast-address {add | remove} {ethernet interface-list | port-channel port-channel-list}

no bridge multicast ipv6 forbidden source ipv6-address group ipv6-multicast-address
```

Parameters

- `ipv6-source-address`—Specifies the source IPv6 address.
- `ipv6-multicast-address`—Specifies the group IPv6 multicast address.
- `add`—Forbids adding ports to the group for the specific source IPv6 address.
- `remove`—Forbids removing ports from the group for the specific source IPv6 address.
- `ethernet interface-list`—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.
Default Configuration
No forbidden addresses are defined.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Before defining forbidden ports, the Multicast group should be registered.
You can execute the command before the VLAN is created.

Example
The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table, and forbids adding the pair to gi1/1/9 on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:4:4:4:1 group FF00:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast forbidden source 2001:0:0:4:4:4:1 group FF00:0:0:4:4:4:1 add gi1/1/9
```

31.14 bridge multicast unregistered
Use the `bridge multicast unregistered` Interface Configuration (Ethernet, Port-Channel) mode command to configure forwarding unregistered Multicast addresses. Use the `no` form of this command to restore the default configuration.

Syntax

```
bridge multicast unregistered [forwarding | filtering]
no bridge multicast unregistered
```

Parameters
- `forwarding`—Forwards unregistered Multicast packets.
- `filtering`—Filters unregistered Multicast packets.
**Default Configuration**

Unregistered Multicast addresses are forwarded.

**Command Mode**

Interface Configuration (Ethernet, Port-Channel) mode

**User Guidelines**

Do not enable unregistered Multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

**Example**

The following example specifies that unregistered Multicast packets are filtered on gi1/1/1:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# bridge multicast unregistered filtering
```

**31.15 bridge multicast forward-all**

Use the `bridge multicast forward-all` Interface Configuration (VLAN) mode command to enable forwarding all multicast packets for a range of ports or port channels. Use the no form of this command to restore the default configuration.

**Syntax**

```
bridge multicast forward-all [add | remove] {ethernet interface-list | port-channel port-channel-list}
no bridge multicast forward-all
```

**Parameters**

- `add`—Forces forwarding of all Multicast packets.
- `remove`—Does not force forwarding of all Multicast packets.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**
Forwarding of all Multicast packets is disabled.

**Command Mode**
Interface Configuration (VLAN) mode

**Example**
The following example enables all Multicast packets on port gi1/1/8 to be forwarded.

```
switchxxxxx(config)# interface vlan 2
switchxxxxx(config-if)# bridge multicast forward-all add gi1/1/8
```

### 31.16 bridge multicast forbidden forward-all

Use the `bridge multicast forbidden forward-all` Interface Configuration (VLAN) mode command to forbid a port to dynamically join Multicast groups. Use the no form of this command to restore the default configuration.

**Syntax**

`bridge multicast forbidden forward-all [add | remove] [ethernet interface-list | port-channel port-channel-list]`

`no bridge multicast forbidden forward-all`

**Parameters**

- **add**—Forbids forwarding of all Multicast packets.
- **remove**—Does not forbid forwarding of all Multicast packets.
- `ethernet interface-list` — Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- `port-channel port-channel-list` — Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

Ports are not forbidden to dynamically join Multicast groups.

The default option is `add`.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Use this command to forbid a port to dynamically join (by IGMP, for example) a Multicast group.

The port can still be a Multicast router port.

**Example**

The following example forbids forwarding of all Multicast packets to gi1/1/1 within VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forbidden forward-all add ethernet gi1/1/1
```

### 31.17 bridge unicast unknown

Use the `bridge unicast unknown` Interface Configuration (Ethernet, port-channel) mode command to enable egress filtering of Unicast packets where the destination MAC address is unknown to the device. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
bridge unicast unknown {filtering | forwarding}
```
no bridge unicast unknown

Parameters

- filtering— Filter unregistered Unicast packets.
- forwarding— Forward unregistered Unicast packets.

Default Configuration

Forwarding.

Command Mode

Interface Configuration (Ethernet, port-channel) mode.

Example

The following example drops Unicast packets on gi1/1/1 when the destination is unknown.

```
switchxxxxxxx(config)# interface gi1/1/1
switchxxxxxxx(config-if)# bridge unicast unknown filtering
```

31.18 show bridge unicast unknown

Use the `show bridge unicast unknown` command to display the unknown Unicast filtering configuration.

Syntax

```
show bridge unicast unknown [interface-id]
```

Parameters

- interface-id— Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

Default

Command Mode

EXEC
Example

Console # show bridge unicast unknown

<table>
<thead>
<tr>
<th>Port</th>
<th>Unregistered</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>--------------</td>
</tr>
<tr>
<td>1/1</td>
<td>Forward</td>
</tr>
<tr>
<td>1/2</td>
<td>Filter</td>
</tr>
<tr>
<td>1/3</td>
<td>Filter</td>
</tr>
</tbody>
</table>

31.19  mac address-table static

Use the `mac address-table static` Global Configuration mode command to add a MAC-layer station source address to the MAC address table. Use the `no` form of this command to delete the MAC address.

Syntax

```
mac address-table static mac-address vlan vlan-id interface interface-id [permanent /delete-on-reset /delete-on-timeout /secure]
no mac address-table static [mac-address] vlan vlan-id
```

Parameters

- `mac-address`— MAC address (Range: Valid MAC address)
- `vlan-id`— Specify the VLAN
- `interface-id`— Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: valid ethernet port, valid port-channel)
- `permanent`— The permanent static MAC address. The keyword is applied by the default.
- `delete-on-reset`— The delete-on-reset static MAC address.
- `delete-on-timeout`— The delete-on-timeout static MAC address.
- `secure`— The secure MAC address. May be used only in a secure mode.
Default Configuration
No static addresses are defined. The default mode for an added address is permanent.

Command Mode
Global Configuration mode

User Guidelines
Use the command to add a static MAC address with given time-to-live in any mode or to add a secure MAC address in a secure mode.

Each MAC address in the MAC address table is assigned two attributes: type and time-to-live.

The following value of time-of-live is supported:

- permanent— a MAC address is saved until it is removed manually.
- delete-on-reset— a MAC address is saved until the next reboot.
- delete-on-timeout— a MAC address that may be removed by the aging timer.

The following types are supported:

- static— MAC address manually added by the command with the following keywords specifying its time-of-live:
  - permanent
  - delete-on-reset
  - delete-on-timeout
  A static MAC address may be added in any port mode.

- secure— A MAC address added manually or learned in a secure mode. Use the mac address-table static command with the secure keyword to add a secure MAC address. The MAC address cannot be relearned.
  A secure MAC address may be added only in a secure port mode.

- dynamic— a MAC address learned by the switch in non secure mode. A value of its time-to-live attribute is delete-on-timeout.
Examples

Example 1 - The following example adds two permanent static MAC address:

```
switchxxxxxx(conf)#mac address-table static 00:3f:bd:45:5a:b1 vlan 1 interface gi1/1/1
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/1/1 permanent
```

Example 2 - The following example adds a deleted-on-reset static MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/1/1 delete-on-reset
```

Example 3 - The following example adds a deleted-on-timeout static MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/1/1 delete-on-timeout
```

Example 4 - The following example adds a secure MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/1/1 secure
```

31.20 clear mac address-table

Use the clear mac address-table Privileged EXEC command to remove learned or secure entries from the forwarding database (FDB).

Syntax

```
clear mac address-table dynamic interface interface-id

clear mac address-table secure interface interface-id
```
Parameters

- **dynamic interface interface-id**—Delete all dynamic (learned) addresses on the specified interface. The interface ID can be one of the following types: Ethernet port or port-channel. If interface ID is not supplied, all dynamic addresses are deleted.

- **secure interface interface-id**—Delete all the secure addresses learned on the specific interface. A secure address on a MAC address learned on ports on which port security is defined.

**Default Configuration**

For dynamic addresses, if interface-id is not supplied, all dynamic entries are deleted.

**Command Mode**

Privileged EXEC mode

**Examples:**

**Example 1** - Delete all dynamic entries from the FDB.

```plaintext
switchxxxxxx# clear mac address-table dynamic
```

**Example 2** - Delete all secure entries from the FDB learned on secure port gi1.

```plaintext
switchxxxxxx# clear mac address-table secure interface gi1
```

### 31.21 mac address-table aging-time

Use the `mac address-table aging-time` Global configuration command to set the aging time of the address table. Use the `no` form of this command to restore the default.

**Syntax**

- `mac address-table aging-time seconds`
- `no mac address-table aging-time`
31.22 port security

Use the port security Interface Configuration (Ethernet, Port-channel) mode command to enable port security learning mode on an interface. Use the no form of this command to disable port security learning mode on an interface.

Syntax

port security [forward / discard / discard-shutdown] [trap seconds]

no port security

Parameters

- **forward**—Forwards packets with unlearned source addresses, but does not learn the address.
- **discard**—Discards packets with unlearned source addresses.
- **discard-shutdown**—Discards packets with unlearned source addresses and shuts down the port.
- **trap seconds**—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration

The feature is disabled by default.

The default mode is **discard**.
The default number of seconds is zero, but if **traps** is entered, a number of seconds must also be entered.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

See the **bridge unicast unknown** command for information about MAC address attributes (type and time-to-live) definitions.

When the **port security** command enables the **lock** mode on a port all dynamic addresses learned on the port are changed to **permanent secure** addresses.

When the **port security** command enables a mode on a port differing from the **lock** mode all dynamic addresses learned on the port are deleted.

When the **no port security** command cancels a secure mode on a port all secure addresses defined on the port are changed to **dynamic** addresses.

Additionally to set a mode, use the **port security** command to set an action that the switch should perform on a frame which source MAC address cannot be learned.

**Example**

The following example forwards all packets to port gi1/1/1 without learning addresses of packets from unknown sources and sends traps every 100 seconds, if a packet with an unknown source address is received.

```
switchxxxxxx(config)interface gi1/1/7
switchxxxxxx(config-if)port security mode lock
switchxxxxxx(config-if)port security forward trap 100
switchxxxxxx(config-if)exit
```

### 31.23 port security mode

Use the **port security mode** Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the **no** form of this command to restore the default configuration.
Syntax

port security mode {max-addresses | lock | secure permanent | secure delete-on-reset}

no port security mode

Parameters

- **max-addresses**— Non secure mode with limited learning dynamic MAC addresses. The static MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

- **lock**— Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

- **secure permanent**— Secure mode with limited learning permanent secure MAC addresses with the `permanent` time-of-live. The static and secure MAC addresses may be added on the port manually by the `mac address-table static` command.

- **secure delete-on-reset**— Secure mode with limited learning secure MAC addresses with the `delete-on-reset` time-of-live. The static and secure MAC addresses may be added on the port manually by the `mac address-table static` command.

Default Configuration

The default port security mode is **lock**.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses. The static MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use the `port security mode` command to change the default mode before the `port security mode` command.
Example

The following example sets the port security mode to Lock for gi1/1/7.

```
switchxxxxx(config) interface gi1/1/7
switchxxxxx(config-if) port security mode lock
switchxxxxx(config-if) port security
switchxxxxx(config-if) exit
```

31.24 port security max

Use the `port security max` Interface Configuration (Ethernet, Port-channel) mode command to configure the maximum number of addresses that can be learned on the port while the port is in port, max-addresses or secure mode. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
port security max max-addr
no port security max
```

**Parameters**

- `max-addr`—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–256)

**Default Configuration**

This default maximum number of addresses is 1.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use this command to change the default value before the `port security` command.
Example
The following example sets the port to limited learning mode:

```
switchxxxxxx(config)#interface gi7
switchxxxxxx(config-if)port security mode max
switchxxxxxx(config-if)port security max 20
switchxxxxxx(config-if)port security
switchxxxxxx(config-if)exit
```

### 31.25 show mac address-table

Use the `show mac address-table` EXEC command to view entries in the MAC address table.

**Syntax**

```
show mac address-table [dynamic | static | secure] [vlan vlan] [interface interface-id] [address mac-address]
```

**Parameters**

- `dynamic`—Displays only dynamic MAC address table entries.
- `static`—Displays only static MAC address table entries.
- `secure`—Displays only secure MAC address table entries.
- `vlan`—Displays entries for a specific VLAN.
- `interface-id`—Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `mac-address`—Displays entries for a specific MAC address.

**Default Configuration**

If no parameters are entered, the entire table is displayed.

**Command Mode**

EXEC mode
User Guidelines

Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

Example

Example 1 - Displays entire address table.

```bash
switchxxxxxx# show mac address-table
Flags: I - Internal usage VLAN
Aging time is 300 sec

VLAN    MAC Address         Port       Type
-------- --------------------- ---------- ----------
 1       00:00:26:08:13:23       0       self
 1       00:3f:bd:45:5a:b1     gi1/1/1       static
 1       00:a1:b0:69:63:f3     gi1/1/4       dynamic
 2       00:a1:b0:69:63:f3     gi1/1/5       dynamic
gi7(I)   00:a1:b0:69:61:12     gi7       dynamic
```

Example 2 - Displays address table entries containing the specified MAC address.

```bash
switchxxxxxx# show mac address-table address 00:3f:bd:45:5a:b1
Flags: I - Internal usage VLAN
Aging time is 300 sec

VLAN    MAC Address Port Type
-------- --------------------- ---------- ----------
   1     00:3f:bd:45:5a:b1 gi1/1/9 static
```

31.26 show mac address-table count

Use the `show mac address-table count` EXEC mode command to display the number of addresses present in the Forwarding Database.

Syntax

`show mac address-table count [vlan vlan | interface interface-id]`
Parameters

- **vlan**—Specifies VLAN.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show mac address-table count
This may take some time.
Capacity : 16384
Free     : 16379
Used     : 5
Secure   : 0
Dynamic  : 2
Static   : 2
Internal : 1
console#
```

**31.27 show bridge multicast mode**

Use the `show bridge multicast mode` EXEC mode command to display the Multicast bridging mode for all VLANs or for a specific VLAN.

Syntax

```
show bridge multicast mode [vlan vlan-id]
```

Parameters

- **vlan vlan-id**—Specifies the VLAN ID.

Command Mode

EXEC mode
Example

The following example displays the Multicast bridging mode for all VLANs.

```
switchxxxxxxx# show bridge multicast mode
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IPv4 Multicast Mode</th>
<th>IPv6 Multicast Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Admin</td>
<td>Oper</td>
</tr>
<tr>
<td>---</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>1</td>
<td>MAC-GROUP</td>
<td>MAC-GROUP</td>
</tr>
<tr>
<td>11</td>
<td>IPv4-GROUP</td>
<td>IPv4-GROUP</td>
</tr>
<tr>
<td>12</td>
<td>IPv4-SRC-GROUP</td>
<td>IPv6-SRC-GROUP</td>
</tr>
</tbody>
</table>

31.28  show bridge multicast address-table

Use the `show bridge multicast address-table` EXEC mode command to display Multicast MAC addresses or IP Multicast address table information.

Syntax

```
show bridge multicast address-table [vlan vlan-id] [address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}] [format {ip | mac}] [source {ipv4-source-address | ipv6-source-address}]
```

Parameters

- `vlan vlan-id`—Display entries for specified VLAN ID.
- `address`—Display entries for specified Multicast address. The possible values are:
  - `mac-multicast-address`—Specifies the MAC Multicast address.
  - `ipv4-multicast-address`—Specifies the IPv4 Multicast address.
  - `ipv6-multicast-address`—Specifies the IPv6 Multicast address.
- `format`—(this applies if picked mac-multicast-address). then i can display it either in mac or ip format) Display entries for specified Multicast address format. The possible values are:
  - `ip`—Specifies that the Multicast address is an IP address.
  - `mac`—Specifies that the Multicast address is a MAC address.
source {ipv4-source-address | ipv6-source-address}—Specifies the source address. The possible values are:
- ipv4-address—Specifies the source IPv4 address.
- ipv6-address—Specifies the source IPv6 address.

Default Configuration

If the format is not specified, it defaults to mac (only if mac-multicast-address was entered).

If VLAN ID is not entered, entries for all VLANs are displayed.

If MAC or IP address is not supplied, entries for all addresses are displayed.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast router ports (defined statically or discovered dynamically) are members in all MAC groups.

Ports that were defined via the bridge multicast forbidden forward-all command are displayed in all forbidden MAC entries.

Changing the Multicast mode can move static Multicast addresses that are written in the device FDB to a shadow configuration because of FDB hash collisions.

Example

The following example displays bridge Multicast address information.

switchxxxxxx# show bridge multicast address-table

Multicast address table for VLANs in MAC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>01:00:5e:02:02:03</td>
<td>Static</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Multicast address table for VLANs in IPv4-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224.0.0.251</td>
<td>Dynamic</td>
<td>gi1/1/2</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>232.5.6.5</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>233.22.2.6</td>
<td></td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224.2.2.251</td>
<td>11.2.2.3</td>
<td>Dynamic</td>
<td>gi1/1/1</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>239.2.2.2</td>
<td>*</td>
<td>gi1/1/9</td>
</tr>
<tr>
<td>8</td>
<td>239.2.2.2</td>
<td>1.1.1.11</td>
<td>gi1/1/9</td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv6-GROUP bridging mode:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>Static</td>
<td>gi1/1/1-2, gi1/1/7, Pol</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>gi1/1/9</td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>*</td>
<td>Static</td>
<td>gi1/1/1-2,gi1/1/7,Pol</td>
</tr>
</tbody>
</table>
Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>*</td>
<td>gi1/1/9</td>
</tr>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>fe80::200:7ff:</td>
<td>gi1/1/9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e00:200</td>
<td></td>
</tr>
</tbody>
</table>

### 31.29 `show bridge multicast address-table static`

Use the `show bridge multicast address-table static` EXEC mode command to display the statically configured Multicast addresses.

**Syntax**

```
show bridge multicast address-table static [vlan vlan-id] [address mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address] [source ipv4-source-address | ipv6-source-address] [all | mac | ip]
```

**Parameters**

- **vlan vlan-id**—Specifies the VLAN ID.
- **address**—Specifies the Multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC Multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 Multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 Multicast address.
- **source**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

**Default Configuration**

When all/mac/ip is not specified, all entries (MAC and IP) will be displayed.
Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000-- 0100.5e7f.ffff.

Example

The following example displays the statically configured Multicast addresses.

```
switchxxxxxx# show bridge multicast address-table static

MAC-GROUP table
Vlan  MAC Address  Ports
----  --------------  ------
  1    0100.9923.8787  gi1/1/1, gi1/1/2

Forbidden ports for multicast addresses:
Vlan  MAC Address  Ports
----  --------------  ------

IPv4-GROUP Table
Vlan  IP Address    Ports
----  ---------      ------
  1    231.2.2.3     gi1/1/1, gi1/1/2
  19   231.2.2.8     gi1/1/8
  19   231.2.2.8     gi1/1/3

Forbidden ports for multicast addresses:
Vlan  IP Address    Ports
----  ---------      ------
  1    231.2.2.3     gi1/1/8
  19   231.2.2.8     gi1/1/3

IPv4-SRC-GROUP Table:
Vlan  Group Address  Source address  Ports
----  ---------------  --------------  ------

Forbidden ports for multicast addresses:
```
### Show Bridge Multicast Filtering

Use the `show bridge multicast filtering` EXEC mode command to display the Multicast filtering configuration.

**Syntax**

`show bridge multicast filtering vlan-id`

**Parameters**

- `vlan-id`—Specifies the VLAN ID. (Range: Valid VLAN)
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays the Multicast configuration for VLAN 1.

```
switchxxxxxx# show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1
Forward-All
Port Static Status
----- -------- ------
gi1/1/1 Forbidden Filter
gi1/1/2 Forward Forward(s)
gi1/1/3 - Forward(d)
```

31.31  show bridge multicast unregistered

Use the `show bridge multicast unregistered` EXEC mode command to display the unregistered Multicast filtering configuration.

Syntax
show bridge multicast unregistered [interface-id]

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
Display for all interfaces.
### Command Mode
EXEC mode

### Example
The following example displays the unregistered Multicast configuration.

```
switchxxxxxx# show bridge multicast unregistered
Port     Unregistered
--------- --------------
gi1/1/1   Forward
        Filter
        Filter
```

### 31.32 show ports security

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

#### Syntax
`show ports security [interface-id | detailed]`

#### Parameters
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `detailed`—Displays information for non-present ports in addition to present ports.

#### Default Configuration
Display for all interfaces. If detailed is not used, only present ports are displayed.

#### Command Mode
Privileged EXEC mode
Example

The following example displays the port-lock status of all ports.

```
switchxxxxxx# show ports security
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Action</th>
<th>Maximum</th>
<th>Trap</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>Max-</td>
<td>Discard</td>
<td>3</td>
<td>Enabled</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Disabled</td>
<td>Max-</td>
<td></td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Enabled</td>
<td>Lock</td>
<td>Discard,</td>
<td>8</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shutdown</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table describes the fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Status</td>
<td>The port security status. The possible values are: Enabled or Disabled.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken on violation.</td>
</tr>
<tr>
<td>Maximum</td>
<td>The maximum number of addresses that can be associated on this port in the Max-Addresses mode.</td>
</tr>
<tr>
<td>Trap</td>
<td>The status of SNMP traps. The possible values are: Enable or Disable.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The minimum time interval between consecutive traps.</td>
</tr>
</tbody>
</table>

31.33  show ports security addresses

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

Syntax

```
show ports security addresses [interface-id | detailed]
```
Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked port:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Current</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>gi2</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi3</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi4</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi5</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi6</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi7</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

31.34  **bridge multicast reserved-address**

Use the **bridge multicast reserved-address** Global Configuration mode command to define the action on Multicast reserved-address packets. Use the **no** form of this command to revert to default.
Syntax

```
bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype /
llc sap / llc-snap pid] [discard | bridge]
```

```
no bridge multicast reserved-address mac-multicast-address [ethernet-v2
ethtype / llc sap / llc-snap pid]
```

Parameters

- **mac-multicast-address**—MAC Multicast address in the reserved MAC addresses range.(Range: 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-2F)
- **ethernet-v2 ethtype**—Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format).(Range: 0x0600–0xFFFF)
- **llc sap**—Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format).(Range: 0xFFFF)
- **llc-snap pid**—Specifies that the packet type is LLC-SNAP and the PID field (40 bits in hexadecimal format). (Range: 0x0000000000 - 0xFFFFFFFFFF)
- **discard**—Specifies discarding the packets.
- **bridge**—Specifies bridging (forwarding) the packets

Default Configuration

- If the user-supplied MAC Multicast address, ethertype and encapsulation (LLC) specifies a protocol supported on the device (called Peer), the default action (discard or bridge) is determined by the protocol.
- If not, the default action is as follows:
  - For MAC addresses in the range 01-80-C2-00-00-00, 01-80-C2-00-00-02– 01-80-C2-00-00-0F, the default is discard.
  - For MAC addresses in the range 00-80-C2-00-00-10– 01-80-C2-00-00-2F, the default is bridge.

Command Mode

Global Configuration mode

User Guidelines

If the packet/service type (ethertype/encapsulation) is not specified, the configuration is relevant to all the packets with the configured MAC address.
Specific configurations (that contain service type) have precedence over less specific configurations (contain only MAC address).

The packets that are bridged are subject to security ACLs.

The actions define by this command has precedence over forwarding rules defined by applications/protocols (STP, LLDP etc.) supported on the device.

Example

```
switchxxxxxx(conf)#bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

### 31.35 show bridge multicast reserved-addresses

Use the **show bridge multicast reserved-addresses** EXEC mode command to display the Multicast reserved-address rules.

**Syntax**

```
show bridge multicast reserved-addresses
```

**Command Mode**

EXEC mode

**Example**

```
switchxxxxxx # show bridge multicast reserved-addresses
```

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Frame Type</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>LLC-SNAP</td>
<td>00-00-0C-01-29</td>
<td>Bridge</td>
</tr>
</tbody>
</table>
### 32.1 port monitor

Use the `port monitor` Interface Configuration (Ethernet) mode command to start a port monitoring session (mirroring). Use the `no` form of this command to stop a port monitoring session.

**Syntax**

```plaintext
port monitor src-interface-id [rx | tx]
no port monitor src-interface-id
port monitor vlan vlan-id
no port monitor vlan vlan-id
```

**Parameters**

- `rx`—Monitors received packets only. If no option is specified, it monitors both `rx` and `tx`.
- `tx`—Monitors transmitted packets only. If no option is specified, it monitors both `rx` and `tx`.
- `vlan vlan-id`—VLAN number
- `src-interface-id`—Specifies an interface ID. The interface ID must be an Ethernet port.

**Default Configuration**

Monitors both received and transmitted packets.

**Command Mode**

Interface Configuration (Ethernet) mode. It cannot be configured for a range of interfaces (range context).

**User Guidelines**

This command enables port copy between Source Port (src-interface) to a Destination Port (The port in context).
The analyzer port for port ingress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for port egress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for VLAN mirroring should be the same for all the mirrored VLANs, and should be the same port as the analyzer port for port ingress mirroring traffic.

The following restriction applies to ports that are configured to be source ports:

- The port cannot be a destination port.

The following restrictions apply to ports that are configured to be monitor ports:

- The port cannot be source port.
- The port is not a member in port-channel.
- IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will be automatically removed from the default VLAN).
- L2 protocols, such as: LLDP, CDP, LBD, STP, LACP, are not active on the destination port.

Notes:

1. In this mode some traffic duplication on the analyzer port may be observed. For example:
   - Port 2 is being egress monitored by port 4.
   - Port 2 & 4 are members in VLAN 3.
   - Unknown Unicast packet sent to VLAN 3 will egress from port 4 twice, one instance as normal forward and another instance as mirrored from port 2.
   - Moreover, if port 2 is an untagged member in VLAN 3 and port 4 is a tagged member then both instances will look different (one tagged and the other is not).

1. When the port is configured to 802.1X auto mode it will forward any mirrored traffic regardless of the.1X state. However, it will operate as a normal network port (forward traffic) only after authorization is done.
2. Mirrored traffic is exposed to STP state, i.e. if the port is in STP blocking, it will not egress any mirrored traffic.

**Example**

The following example copies traffic for both directions (Tx and Rx) from the source port gi1/1/2 to destination port gi1/1/1.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# port monitor gi1/1/2
```

### 32.2 show ports monitor

Use the `show ports monitor` EXEC mode command to display the port monitoring status.

**Syntax**

`show ports monitor`

**Command Mode**

EXEC mode

**Example**

The following example displays the port monitoring status.

```
switchxxxxxx# show ports monitor

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination Port</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/8</td>
<td>gi1/1/1</td>
<td>RX,TX</td>
<td>Active</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>gi1/1/1</td>
<td>RX,TX</td>
<td>Active</td>
</tr>
<tr>
<td>gi1/1/18</td>
<td>gi1/1/1</td>
<td>Rx</td>
<td>Active</td>
</tr>
</tbody>
</table>
```
Spanning-Tree Commands

33.1 spanning-tree

Use the `spanning-tree` Global Configuration mode command to enable spanning-tree functionality. Use the `no` form of this command to disable the spanning-tree functionality.

**Syntax**

```
spanning-tree
no spanning-tree
```

**Parameters**

N/A

**Default Configuration**

Spanning-tree is enabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables spanning-tree functionality.

```
switchxxxxxx(config)# spanning-tree
```

33.2 spanning-tree mode

Use the `spanning-tree mode` Global Configuration mode command to select which Spanning Tree Protocol (STP) protocol to run. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
spanning-tree mode {stp / rstp / mst}
```
no spanning-tree mode

Parameters

- **stp**—Specifies that STP is enabled.
- **rstp**—Specifies that the Rapid STP is enabled.
- **mst**— Specifies that the Multiple STP is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example enables MSTP.

```
switchxxxxxx(config)# spanning-tree mode mst
```

### 33.3 spanning-tree forward-time

Use the `spanning-tree forward-time` Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
spanning-tree forward-time seconds
no spanning-tree forward-time
```
Parameters

**seconds**—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

\[ 2 \times (\text{Forward-Time} - 1) \geq \text{Max-Age} \]

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
switchxxxxxx(config)# spanning-tree forward-time 25
```

### 33.4 spanning-tree hello-time

Use the `spanning-tree hello-time` Global Configuration mode command to configure how often the device broadcasts Hello messages to other devices. Use the `no` form of this command to restore the default configuration.

Syntax

```
spanning-tree hello-time seconds
no spanning-tree hello-time
```

Parameters

**seconds**—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration

2 seconds.
Command Mode
Global Configuration mode

User Guidelines
When configuring the Hello time, the following relationship should be maintained:

\[
\text{Max-Age} \geq 2 \times (\text{Hello-Time} + 1)
\]

Example
The following example configures the spanning-tree bridge hello time to 5 seconds.

```
switchxxxxxx(config)# spanning-tree hello-time 5
```

33.5 spanning-tree max-age

Use the `spanning-tree max-age` Global Configuration mode command to configure the STP maximum age. Use the `no` form of this command to restore the default configuration.

Syntax

```
spanning-tree max-age seconds
no spanning-tree max-age
```

Parameters

`seconds`—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration

The default maximum age is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be maintained:
2*(Forward-Time - 1) >= Max-Age
Max-Age >= 2*(Hello-Time + 1)

Example
The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
switchxxxxx(config)# spanning-tree max-age 10
```

### 33.6 spanning-tree priority

Use the `spanning-tree priority` Global Configuration mode command to configure the device STP priority, which is used to determine which bridge is selected as the root bridge. Use the `no` form of this command to restore the default device spanning-tree priority.

**Syntax**

```plaintext
spanning-tree priority priority
no spanning-tree priority
```

**Parameters**

- **priority**—Specifies the bridge priority. (Range: 0–61440)

**Default Configuration**

Default priority = 32768.

**Command Mode**

Global Configuration mode

**User Guidelines**

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.
Example

The following example configures the spanning-tree priority to 12288.

switchxxxxxx(config)# spanning-tree priority 12288

33.7 spanning-tree disable

Use the `spanning-tree disable` Interface Configuration (Ethernet, port-channel) mode command to disable the spanning tree on a specific port. Use the `no` form of this command to enable the spanning tree on a port.

Syntax

```
spanning-tree disable
no spanning-tree disable
```

Parameters

N/A

Default Configuration

Spanning tree is enabled on all ports.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example disables the spanning tree on gi1/1/5

switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# spanning-tree disable

33.8 spanning-tree cost

Use the `spanning-tree cost` Interface Configuration (Ethernet, port-channel) mode command to configure the spanning-tree path cost for a port. Use the `no` form of this command to restore the default configuration.
Spanning-Tree Commands

Syntax

spanning-tree cost cost

no spanning-tree cost

Parameters

cost—Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>TenGigabit Ethernet (10000 Mbps)</td>
<td>2000</td>
<td>2</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example configures the spanning-tree cost on gi1/1/15 to 35000.

switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# spanning-tree cost 35000

33.9 spanning-tree port-priority

Use the spanning-tree port-priority Interface Configuration (Ethernet, port-channel) mode command to configure the port priority. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree port-priority priority
no spanning-tree port-priority

Parameters

priority—Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority is 128.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on gi1/1/15 to 96

switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# spanning-tree port-priority 96

33.10 spanning-tree portfast

Use the spanning-tree portfast Interface Configuration (Ethernet, port-channel) mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the no form of this command to disable the PortFast mode.

Syntax

spanning-tree portfast [auto]

no spanning-tree portfast

Parameters

auto—Specifies that the software waits for 3 seconds (with no Bridge Protocol Data Units (BPDUs) received on the interface) before putting the interface into the PortFast mode.
Spanning-Tree Commands

Default Configuration
PortFast mode is disabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example enables the PortFast mode on gi1/1/15.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# spanning-tree portfast
```

33.11 spanning-tree link-type

Use the `spanning-tree link-type` Interface Configuration (Ethernet, port-channel) mode command to override the default link-type setting determined by the port duplex mode, and enable RSTP transitions to the Forwarding state. Use the `no` form of this command to restore the default configuration.

Syntax
```
spanning-tree link-type {point-to-point | shared}
no spanning-tree spanning-tree link-type
```

Parameters
- `point-to-point`—Specifies that the port link type is point-to-point.
- `shared`—Specifies that the port link type is shared.

Default Configuration
The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Mode
Interface Configuration (Ethernet, port-channel) mode
Example
The following example enables shared spanning-tree on gi1/1/15.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# spanning-tree link-type shared
```

### 33.12 spanning-tree pathcost method

Use the `spanning-tree pathcost method` Global Configuration mode command to set the default path cost method. Use the `no` form of this command to return to the default configuration.

**Syntax**

```
spanning-tree pathcost method [long | short]
no spanning-tree pathcost method
```

**Parameters**

- **long**—Specifies that the default port path costs are within the range: 1–200,000,000.
- **short**—Specifies that the default port path costs are within the range: 1–200,000,000.

**Default Configuration**

Long path cost method.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command applies to all the spanning tree instances on the switch.

- If the short method is selected, the switch calculates the default cost as 100.
- If the long method is selected, the switch calculates the default cost as 20000.
Example

The following example sets the default path cost method to Long.

switchxxxxxx(config)# spanning-tree pathcost method long

33.13 spanning-tree bpdu (Global)

Use the spanning-tree bpdu Global Configuration mode command to define Bridge Protocol Data Unit (BPDU) handling when the spanning tree is disabled globally or on a single interface. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree bpdu [filtering | flooding]

no spanning-tree bpdu

Parameters

- filtering—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- flooding—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The default setting is flooding.

Command Mode

Global Configuration mode

User Guidelines

The filtering and flooding modes are relevant when the spanning tree is disabled globally or on a single interface.
Example
The following example defines the BPDU packet handling mode as **flooding** when the spanning tree is disabled on an interface.

```
switchxxxxxx(config)# spanning-tree bpdu flooding
```

### 33.14 spanning-tree bpdu (Interface)

Use the `spanning-tree bpdu` Interface Configuration (Ethernet, Port-channel) mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
spanning-tree bpdu {filtering | flooding}
no spanning-tree bpdu
```

**Parameters**

- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

**Default Configuration**

The `spanning-tree bpdu (Global)` command determines the default configuration.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**Example**

The following example defines the BPDU packet as **flooding** when the spanning tree is disabled on gi1/1/3.

```
switchxxxxxx(config)# interface gi1/1/3
switchxxxxxx(config-if)# spanning-tree bpdu flooding
```
33.15 spanning-tree guard root

Use the `spanning-tree guard root` Interface Configuration (Ethernet, Port-channel) mode command to enable Root Guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the `no` form of this command to disable the root guard on the interface.

**Syntax**

```plaintext
spanning-tree guard root

no spanning-tree guard root
```

**Default Configuration**

Root guard is disabled.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

Root Guard can be enabled when the device operates in any mode (STP, RSTP and MSTP).

When Root Guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

**Example**

The following example prevents gi1/1/1 from being the root port of the device.

```plaintext
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# spanning-tree guard root
```

33.16 spanning-tree bpduguard

Use the `spanning-tree bpduguard` Interface Configuration (Ethernet, port-channel) mode command to shut down an interface when it receives a Bridge Protocol Data Unit (BPDU). Use the `no` form of this command to restore the default configuration.
Syntax

spanning-tree bpduguard \texttt{\{enable \ / disable\}}

no spanning-tree bpduguard

Parameters

\texttt{bpduguard enable}—Enables BPDU Guard.

\texttt{bpduguard disable}—Disables BPDU Guard.

Default Configuration

BPDU Guard is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

Example

The following example shuts down gi1/1/5 when it receives a BPDU.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# spanning-tree bpduguard enable
```

33.17 clear spanning-tree detected-protocols

Use the \texttt{clear spanning-tree detected-protocols} Privileged EXEC command to restart the STP migration process (force renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

\texttt{clear spanning-tree detected-protocols \{interface interface-id\}}
Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This feature can only be used when working in RSTP or MSTP mode.

Example

This restarts the STP migration process on all interfaces.

```
switchxxxxxx# clear spanning-tree detected-protocols
```

33.18 spanning-tree mst priority

Use the spanning-tree mst priority Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the no form of this command to restore the default configuration.

Syntax

```
spanning-tree mst instance-id priority priority
```

```
no spanning-tree mst instance-id priority
```

Parameters

- instance-id—Specifies the spanning-tree instance ID. (Range: 1–15)
- priority—Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)
Default Configuration
The default priority is 32768.

Command Mode
Global Configuration mode

User Guidelines
The priority value must be a multiple of 4096.
The switch with the lowest priority is the root of the spanning tree.

Example
The following example configures the spanning tree priority of instance 1 to 4096.

switchxxxxxxx(config)# spanning-tree mst 1 priority 4096

33.19 spanning-tree mst max-hops
Use the spanning-tree mst max-hops Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the no form of this command to restore the default configuration.

Syntax
spanning-tree mst max-hops  hop-count
no spanning-tree mst max-hops

Parameters
max-hops  hop-count—Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration
The default number of hops is 20.

Command Mode
Global Configuration mode
Example
The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

switchxxxxxx(config)# spanning-tree mst max-hops 10

33.20 spanning-tree mst port-priority
Use the spanning-tree mst port-priority Interface Configuration (Ethernet, port-channel) mode command to configure the priority of a port. Use the no form of this command to restore the default configuration.

Syntax
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority

Parameters
- instance-id—Specifies the spanning tree instance ID. (Range: 1–15)
- priority—Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration
The default port priority is 128.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The priority value must be a multiple of 16.

Example
The following example configures the port priority of gi1/1/1 to 144.

switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# spanning-tree mst 1 port-priority 144
33.21 spanning-tree mst cost

Use the `spanning-tree mst cost` Interface Configuration (Ethernet, Port-channel) mode command to configure the path cost for MST calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost
```

**Default Configuration**

N/A

**Parameters**

- `instance-id`—Specifies the spanning-tree instance ID. (Range: 1–15)
- `cost`—Specifies the port path cost. (Range: 1–200000000)

**Default Configuration**

Default path cost is determined by the port speed and path cost method (long or short) as shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>TenGigabit Ethernet</td>
<td>2000</td>
<td>2</td>
</tr>
<tr>
<td>TenGigabit Ethernet</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Example**

The following example configures the MSTP instance 1 path cost for port gi1/1/9 to 4.
switchxxxxxx(config)# interface gi1/1/9
switchxxxxxx(config-if)# spanning-tree mst 1 cost 4

### 33.22 spanning-tree mst configuration

Use the `spanning-tree mst configuration` Global Configuration mode command to enable configuring an MST region by entering the MST mode.

**Syntax**

```
spanning-tree mst configuration
```

**Command Mode**

Global Configuration mode

**User Guidelines**

For two or more switches to be in the same MST region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

**Example**

The following example configures an MST region.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

### 33.23 instance (MST)

Use `instance` MST Configuration mode command to map VLANs to an MST instance. Use the `no` form of this command to restore the default mapping.

**Syntax**

```
instance instance-id vlan vlan-range
no instance instance-id vlan vlan-range
```
Parameters

- instance-id—MST instance (Range: 1–15)
- vlan-range—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

Default Configuration

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
```

33.24 name (MST)

Use the name MST Configuration mode command to define the MST instance name. Use the no form of this command to restore the default setting.

Syntax

name string
no name
Parameters
string—Specifies the MST instance name. (Length: 1–32 characters)

Default Configuration
The default name is the bridge MAC address.

Command Mode
MST Configuration mode

Example
The following example defines the instance name as Region1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

### 33.25 revision (MST)

Use the `revision` MST Configuration mode command to define the MST configuration revision number. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
revision value
no revision
```

**Parameters**

`value`—Specifies the MST configuration revision number. (Range: 0–65535)

**Default Configuration**

The default configuration revision number is 0.

**Command Mode**

MST Configuration mode
Example
The following example sets the configuration revision to 1.

```
switchxxxxxx(config) # spanning-tree mst configuration
switchxxxxxx(config-mst) # revision 1
```

33.26 show (MST)

Use the `show MST` Configuration mode command to display the current or pending MST region configuration.

Syntax

```
show {current | pending}
```

Parameters

- `current`—Displays the current MST region configuration.
- `pending`—Displays the pending MST region configuration.

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example displays a pending MST region configuration

```
switchxxxxxx(config-mst)# show pending
Gathering information ..........
Current MST configuration
Name: Region1
Revision: 1
Instance   VLANs Mapped          State
---------   ---------------------  -----
```
### 33.27 exit (MST)

Use the `exit` MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

**Syntax**

`exit`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

MST Configuration mode

**Example**

The following example exits the MST Configuration mode and saves changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# exit
switchxxxxxx(config)#
```

### 33.28 abort (MST)

Use the `abort` MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

**Syntax**

`abort`
Parameters
N/A

Default Configuration
N/A

Command Mode
MST Configuration mode

Example
The following example exits the MST Configuration mode without saving changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# abort
```

### 33.29 show spanning-tree

Use the `show spanning-tree` Privileged EXEC mode command to display the spanning-tree configuration.

**Syntax**

```
show spanning-tree [interface-id] [instance instance-id]
show spanning-tree [detail] [active | blockedports] [instance instance-id]
show spanning-tree mst-configuration
```

**Parameters**

- `instance instance-id`—Specifies the spanning tree instance ID. (Range: 1–15)
- `detail`—Displays detailed information.
- `active`—Displays active ports only.
- `blockedports`—Displays blocked ports only.
- `mst-configuration`—Displays the MST configuration identifier.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
**Default Configuration**

If no interface is specified, the default is all interfaces.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

This command only works when MST is enabled.

**Example**

The following examples display spanning-tree information in various configurations:

```plaintext
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID   Priority 32768
          Address 00:01:42:97:e0:00
          Cost    20000
          Port    gi1/1/1
          Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 36864
          Address 00:02:4b:29:7a:00
          Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec
```
### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio. No</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FRW</td>
<td>Root</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority Address
36864 00:02:4b:29:7a:00
This switch is the Root.
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi1/1/5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Root ID Priority Address
N/A N/A
Path Cost N/A
Root Port N/A
Hello Time N/A Max Age N/A Forward Delay N/A
```

### Bridge ID

<table>
<thead>
<tr>
<th>Priority</th>
<th>Address</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>36864</td>
<td>00:02:4b:29:7a:00</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>
Spanning-tree Commands

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nb</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi1/1/5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree active

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID      | Priority | Address                  | Path Cost | Root Port | Hello Time 2 sec | Max Age 20 sec | Forward Delay 15 sec
-------------|----------|--------------------------|-----------|-----------|------------------|----------------|---------------------|
32768        | 00:01:42:97:e0:00 | 20000 | gi1/1/1  |           |                 |                |                     |

Bridge ID    | Priority | Address                  | Hello Time 2 sec | Max Age 20 sec | Forward Delay 15 sec
-------------|----------|--------------------------|------------------|----------------|---------------------|
36864        | 00:02:4b:29:7a:00 |                |                 |                |                     |

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FRW</td>
<td>Root</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree blockedports

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID      | Priority | Address                  | Path Cost | Root Port | Hello Time 2 sec | Max Age 20 sec | Forward Delay 15 sec
-------------|----------|--------------------------|-----------|-----------|------------------|----------------|---------------------|
32768        | 00:01:42:97:e0:00 | 20000 | gi1/1/1  |           |                 |                |                     |
Spanning-T ree Commands

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID  Priority  32768
    Address  00:01:42:97:e0:00
    Path Cost  20000
    Root Port  gi1/1/1
    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago
Times:  hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15

Port 1 (gi1/1/1) enabled
State:  Forwarding  Role:  Root
    Port id: 128.1  Port cost: 20000
    Type: P2p (configured: auto)  RSTP  Port Fast: No (configured:no)
    Designated bridge Priority: 32768  Address: 00:01:42:97:e0:00
    Designated port id: 128.25  Designated path cost: 0
    Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
    BPDU: sent 2, received 120638

Bridge ID  Priority  36864
    Address  00:02:4b:29:7a:00
    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>19</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree detail
Port 2 (gi1/1/2) enabled
State: Forwarding  Role: Designated
Port id: 128.2  Port cost: 20000
Type: Shared (configured: auto) STP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (gi1/1/3) disabled
State: N/A  Role: N/A
Port id: 128.3  Port cost: 20000
Type: N/A (configured: auto)  Port Fast: N/A (configured:no)
Designated bridge Priority: N/A  Address: N/A
Designated port id: N/A  Designated path cost: N/A
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Port 4 (gi1/1/4) enabled
State: Blocking  Role: Alternate
Port id: 128.4  Port cost: 20000
Type: Shared (configured:auto) STP  Port Fast: No (configured:no)
Designated bridge Priority: 28672  Address: 00:30:94:41:62:c8
Designated port id: 128.25  Designated path cost: 20000
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (gi1/1/5) enabled
State: Disabled  Role: N/A
Port id: 128.5  Port cost: 20000
Type: N/A (configured: auto)  Port Fast: N/A (configured:no)
Designated bridge Priority: N/A  Address: N/A
Designated port id: N/A  Designated path cost: N/A
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
switchxxxxxx# **show spanning-tree ethernet** gi1/1/1
Port 1 (gi1/1/1) enabled
State: Forwarding  
Role: Root
Port id: 128.1  
Port cost: 20000
Type: P2p (configured: auto) RSTP  
Port Fast: No (configured:no)
Designated bridge Priority: 32768  
Address: 00:01:42:97:e0:00
Designated port id: 128.25  
Designated path cost: 0
Guard root: Disabled  
BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

switchxxxxxx# **show spanning-tree mst-configuration**
Name: Region1
Revision: 1
Instance  
--------
0  
1
Vlans mapped  
------------
0  
10-20
1  
1-9, 21-4094
State  
--------
Enabled
Enabled

switchxxxxxx# **show spanning-tree**
Spanning tree enabled mode MSTP
Default port cost method: long
#### MST 0 Vlans Mapped: 1-9
CST Root ID  
------------
Priority 32768
Address 00:01:42:97:e0:00
Path Cost 20000
Root Port gi1/1/1
Hello Time 2 sec  
Max Age 20 sec  
Forward Delay 15 sec

IST Master ID  
------------
Priority 32768
Address 00:02:4b:29:7a:00
This switch is the IST master.
Hello Time 2 sec  
Max Age 20 sec  
Forward Delay 15 sec
Max hops 20

Interfaces
### MST 1 Vlans Mapped: 10-20

#### Root ID
- Priority: 24576
- Address: 00:02:4b:29:89:76
- Path Cost: 20000
- Root Port: gi1/1/4
- Rem hops: 19

#### Bridge ID
- Priority: 32768
- Address: 00:02:4b:29:7a:00

#### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FRW</td>
<td>Root</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Enabled</td>
<td>128.3</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FRW</td>
<td>Desg</td>
<td>No</td>
</tr>
</tbody>
</table>

### MST 0 Vlans Mapped: 1-9

#### CST Root ID
- Priority: 32768
- Address: 00:01:42:97:e0:00
- Path Cost: 20000
- Root Port: gi1/1/1

#### IST Master ID
- Priority: 32768
- Address: 00:02:4b:29:7a:00
This switch is the IST master.
Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec
Max hops 20
Number of topology changes 2 last change occurred 2d18h ago
Times:  hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15

Port 1 (gi1/1/1) enabled
State: Forwarding  Role: Root
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:01:42:97:e0:00
Designated port id: 128.25  Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (gi1/1/2) enabled
State: Forwarding  Role: Designated
Port id: 128.2  Port cost: 20000
Type: Shared (configured: auto) Boundary STP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (gi1/1/3) enabled
State: Forwarding  Role: Designated
Port id: 128.3  Port cost: 20000
Type: Shared (configured: auto) Internal  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.3  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Spanning-Tree Commands

Port 4 (gi1/1/4) enabled
State: Forwarding
Role: Designated
Port id: 128.4
Port cost: 20000
Type: Shared (configured: auto) Internal
Port Fast: No (configured:no)
Designated bridge Priority: 32768
Address: 00:02:4b:29:7a:00
Designated port id: 128.2
Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

### MST 1 Vlans Mapped: 10-20

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Rem hops</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24576</td>
<td>00:02:4b:29:89:76</td>
<td>20000</td>
<td>gi1/1/4</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Address</th>
<th>Number of topology changes</th>
<th>Last change occurred</th>
<th>Times:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:02:4b:29:7a:00</td>
<td>2</td>
<td>1d9h</td>
<td>hold 1, topology change 2, notification 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>hello 2, max age 20, forward delay 15</td>
</tr>
</tbody>
</table>

Port 1 (gi1/1/1) enabled
State: Forwarding
Role: Boundary
Port id: 128.1
Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP
Port Fast: No (configured:no)
Designated bridge Priority: 32768
Address: 00:02:4b:29:7a:00
Designated port id: 128.1
Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
Port 2 (gi1/1/2) enabled
State: Forwarding Role: Designated
Port id: 128.2 Port cost: 20000
Type: Shared (configured: auto) Boundary STP Port Fast: No (configured: no)
Designated bridge Priority: 32768 Designated path cost: 20000
Designated port id: 128.2
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (gi1/1/3) disabled
State: Blocking Role: Alternate
Port id: 128.3 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured: no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:1a:19
Designated port id: 128.78 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (gi1/1/4) enabled
State: Forwarding Role: Designated
Port id: 128.4 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured: no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
# MST 0 Vlans Mapped: 1-9

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
<td>20000</td>
<td>gi1/1/1</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
# MST 0 Vlans Mapped: 1-9
33.30  show spanning-tree bpdu

Use the show spanning-tree bpdu EXEC mode command to display the BPDU handling when spanning-tree is disabled.

Syntax

show spanning-tree bpdu [interface-id | detailed]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

- **detailed**—Displays information for non-present ports in addition to present ports.
**Default Configuration**

Show information for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**Example**

The following examples display spanning-tree BPDU information:

```
switchxxxxxx# show spanning-tree bpdu
```

The following is the output if the global BPDU handling command is not supported.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Filtering</td>
<td>Filtering</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Filtering</td>
<td>Filtering</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Filtering</td>
<td>Guard</td>
</tr>
</tbody>
</table>

The following is the output if both the global BPDU handling command and the per-interface BPDU handling command are supported.

Global: Flooding

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Global</td>
<td>Flooding</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Global</td>
<td>STP</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Flooding</td>
<td>STP</td>
</tr>
</tbody>
</table>
Virtual Local Area Network (VLAN) Commands

34.1 vlan database

Use the `vlan database` Global Configuration mode command to enter the VLAN Configuration mode. This mode is used to create VLAN(s) and define the default VLAN.

Use the `exit` command to return to Global Configuration mode.

Syntax

`vlan database`

Parameters

N/A

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example enters the VLAN Configuration mode, creates VLAN 1972 and exits VLAN Configuration mode.

```
switchxxxxxxx(config)# vlan database
switchxxxxxxx(config-vlan)# vlan 1972
switchxxxxxxx(config-vlan)# exit
switchxxxxxxx(config)#
```
### 34.2 vlan

Use the `vlan` VLAN Configuration mode or Global Configuration mode command to create a VLAN. Use the `no` form of this command to delete the VLAN(s).

To assign the VLAN a name, use the Interface Configuration (VLAN) mode `name` command.

**Syntax**

`vlan vlan-range`

`no vlan vlan-range`

**Parameters**

- `vlan-range`—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).

**Default Configuration**

VLAN 1 exists by default.

**Command Mode**

VLAN Configuration mode

**Example**

The following example creates VLANs 100 and 1972.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)#vlan 100,1972
switchxxxxxx(config-vlan)#
```

### 34.3 show vlan

Use the `show vlan` Privileged EXEC mode command to display the following VLAN information for all VLANs or for a specific VLAN:

- VLAN ID
- VLAN name
- Ports on the VLAN
- Whether the VLAN was is dynamic or permanent
- Whether authorization is required on the VLAN

**Syntax**

```
show vlan [tag vlan-id | name vlan-name]
```

**Parameters**

- **tag vlan-id**—Specifies a VLAN ID.
- **name vlan-name**—Specifies a VLAN name string (length: 1–32 characters)

**Default Configuration**

All VLANs are displayed.

**Command Mode**

Privileged EXEC mode

**Examples:**

**Example 1**—The following example displays information for all VLANs:

```
switchxxxxxx# show vlan

Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Created by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default</td>
<td>gi1-2</td>
<td>D</td>
</tr>
<tr>
<td>10</td>
<td>Marketing</td>
<td>gi3-14</td>
<td>S</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>gi5-16</td>
<td>S</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>gi7-18</td>
<td>S</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
<td></td>
<td>S</td>
</tr>
</tbody>
</table>
```
Example 2—The following example displays information for the default VLAN (VLAN 1):

```plaintext
switchxxxxxx# show vlan tag 1
```

Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Created by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default</td>
<td>gi1-2</td>
<td>D</td>
</tr>
</tbody>
</table>

Example 3—The following example displays information for the VLAN named Marketing:

```plaintext
switchxxxxxx# show vlan name Marketing
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Created by</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Marketing</td>
<td>gi3-14</td>
<td>S</td>
</tr>
</tbody>
</table>

### 34.4  `default-vlan vlan`

Use the `default-vlan vlan` VLAN Configuration mode command to define the default VLAN. Use the `no` form of this command to set VLAN 1 as the default VLAN.

**Syntax**

```
default-vlan vlan  vlan-id
no default-vlan vlan
```
Parameters

vlan vlan-id—Specifies the default VLAN ID.

Default Configuration

The default VLAN is 1 by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command becomes effective after reboot of the device.

Example

The following example defines the default VLAN as 2.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# default-vlan vlan 2
```

New Default VLAN ID will be active after save configuration and reboot device.

34.5 show default-vlan-membership

Use the show default-vlan-membership privileged EXEC command to view the default VLAN membership.

Syntax

```
show default-vlan-membership [interface-id | detailed]
```

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—Displays information for non-present ports in addition to present ports.
**Default Configuration**

Membership in the default VLAN is displayed for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

Privileged EXEC

**Example**

```
switchxxxxxx # show default-vlan-membership
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Forbidden</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

---

**34.6 interface vlan**

Use the `interface vlan` Global Configuration mode command to enter the Interface Configuration (VLAN) mode for a specific VLAN. After this command is entered, all commands configure this VLAN. To configure a range of VLANs, use `interface range vlan`.

**Syntax**

`interface vlan vlan-id`

**Parameters**

`vlan vlan-id`—Specifies the VLAN to be configured.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode
**User Guidelines**

If the VLAN does not exist, this command creates it. If the VLAN cannot be created then the command is finished with error and the current context is not changed.

**Example**

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx (config)# interface vlan 1
switchxxxxxx (config-if)# ip address 131.108.1.27 255.255.255.0
```

**34.7  interface range vlan**

Use the `interface range vlan` Global Configuration mode command to configure multiple VLANs simultaneously.

**Syntax**

```
interface range vlan vlan-range
```

**Parameters**

`vlan vlan-range`—Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**User Guidelines**

Commands under the interface VLAN range context are executed independently on each VLAN in the range. If the command returns an error on one of the VLANs, an error message is displayed, and the system attempts to configure the remaining VLANs.
User Guidelines

If the VLAN does not exist, this command creates it. If the VLAN cannot be created then the command is finished with error and the current context is not changed.

Example

The following example groups VLANs 221 through 228 and 889 to receive the same command(s).

```
switchxxxxxx(config)# interface range vlan 221-228, vlan 889
switchxxxxxx(config-if)#
```

34.8 name

Use the `name` Interface Configuration (VLAN) mode command to name a VLAN. Use the `no` form of this command to remove the VLAN name.

Syntax

```
name string
no name
```

Parameters

`string`—Specifies a unique name associated with this VLAN. (Length: 1–32 characters)

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

The VLAN name must be unique.
Example
The following example assigns VLAN 19 the name Marketing.

```
switchxxxxxx(config)# interface vlan 19
switchxxxxxx(config-if)# name Marketing
```

34.9 switchport protected-port

Use the `switchport protected-port` Interface Configuration mode command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports on the same switch. Use the `no` form of this command to disable protection on the port.

Syntax
```
switchport protected-port
no switchport protected-port
```

Parameters
N/A

Default Configuration
Unprotected

Command Mode
Interface configuration (Ethernet, port-channel)

User Guidelines
Note that packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Use this command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules. Use the `switchport community` Interface Configuration command to associate the interface with a community.

Example
switchxxxxxx(config)# interface gi1/1
switchxxxxxx(config-if)# switchport protected-port

34.10  show interfaces protected-ports

Use the show interfaces protected-ports EXEC mode command to display protected ports configuration.

Syntax

show interfaces protected-ports [interface-id | detailed]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

Show all protected interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

switchxxxxxx#show interfaces protected-ports

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Protected</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Protected</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>Unprotected</td>
</tr>
</tbody>
</table>
34.11 switchport mode

Use the `switchport mode` Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN membership mode (access, trunk, general, private-vlan promiscuous, private-vlan host or customer) of a port. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
switchport mode {access | trunk | general | customer}
no switchport mode
```

**Parameters**

- `access`—Specifies an untagged layer 2 VLAN port.
- `trunk`—Specifies a trunking layer 2 VLAN port.
- `general`—Specifies a full 802-1q-supported VLAN port.
- `customer`—Specifies that the port is connected to customer equipment. Used when the switch is in a provider network.

**Default Configuration**

Trunk mode.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- When the port’s mode is changed, it receives the configuration corresponding to the mode.
- If the port mode is changed to access and the access VLAN does not exist, then the port does not belong to any VLAN.
- Trunk and general mode ports can be changed to access mode only if all VLANs (except for an untagged PVID are first removed.
Example

Example 1 - The following example configures gi1/1/1 as an access port (untagged layer 2) VLAN port.

switchxxxxxxx(config)# interface gi1/1/1
switchxxxxxxx(config-if)# switchport mode access
switchxxxxxxx(config-if)# switchport access vlan 2

34.12 switchport access vlan

An interface in access mode can belong to only one VLAN. The switchport access vlan Interface Configuration command reassigns an interface to a different VLAN than it currently belongs to.

Use the no form of this command to restore the default configuration.

Syntax

switchport access vlan vlan-id

no switchport access vlan

Parameters

vlan vlan-id—Specifies the VLAN ID to which the port is configured.

Default Configuration

The interface belongs to the default VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from its previous VLAN and adds it to the new VLAN.

If the interface is a forbidden member of the added VLAN, the interface does not become a member of this VLAN. The system displays an error message about this ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once.").
Example

The following example sets gi1 as an access port and assigns it to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxx(config)# interface gi1/1/2
switchxxxxx(config-if)# switchport mode access
switchxxxxx(config-if)# switchport access vlan 2
```

34.13 switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be a tagged member of one or more VLANs. The `switchport trunk allowed vlan` Interface Configuration mode command adds/removes VLAN(s) to/from a trunk port.

Syntax

```
switchport trunk allowed vlan [add vlan-list | remove vlan-list]
```

Parameters

- **add vlan-list**—Specifies a list of VLAN IDs to add to a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **remove vlan-list**—Specifies a list of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

Default Configuration

By default, trunk ports belongs to the default VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. The system displays an error message about this issue ("An interface cannot become a member of a forbidden VLAN.


This message will only be displayed once, and the command continues to execute in case there are more VLANs in the vlan-list.

Example

To add VLANs 2,3 and 100 to trunk ports 1 to 13:

```
switchxxxxxx(config)# interface range gi1/1/1-13
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
```

34.14 switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port’s native VLAN. Use the switchport trunk native vlan Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN for a trunk interface. Use the no form of this command to restore the default native VLAN.

Syntax

switchport trunk native vlan vlan-id

no switchport trunk native vlan

Parameters

- vlan-id—Specifies the native VLAN ID.

Default Configuration

The default VLAN is the native VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command adds the port as a member of the VLAN. If the port is already a member of the VLAN (not a native), it must first be removed from the VLAN.

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this
case ("An interface cannot become a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute if there are more VLANs in the vlan-list.

Examples:

Example 1 - The following example:

- Defines VLAN 2 as native VLAN for port 1
- Removes VLAN 2 from port 1 and then sets it as the native VLAN

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport trunk native vlan 2
Port 1: Port is Trunk in VLAN 2.
switchxxxxxx(config-if)# switchport trunk allowed vlan remove 2
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

Example 2 - The following example sets packets on port as untagged on ingress and untagged on egress:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

Example 3 - The following example sets packets on port as tagged on ingress and tagged on egress:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2
switchxxxxxx(config-if)#
```
34.15 switchport general allowed vlan

General ports can receive tagged or untagged packets. Use the `switchport general allowed vlan` Interface Configuration mode command to add/remove VLANs to/from a general port and configure whether packets on the egress are tagged or untagged. Use the `no` form of this command to reset to the default.

**Syntax**

```
switchport general allowed vlan {[add vlan-list [tagged | untagged]] | [remove vlan-list]}
```

**Parameters**

- **add vlan-list**—Specifies the list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **tagged**—Specifies that the port transmits tagged packets for the VLANs. This is the default value
- **untagged**— Specifies that the port transmits untagged packets for the VLANs.
- **remove vlan-list**— Specifies the list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

**Default Configuration**

The port is not member in any VLAN.

Packets are transmitted untagged.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

You can change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this case: "An interface cannot become a member of a forbidden VLAN. This
message will only be displayed once.”) and the command continues to execute if there are more VLANs in the vlan-list.

Example

Sets port 1 to general mode and adds VLAN 2 and 3 to it. Packets are tagged on the egress.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

### 34.16 switchport general pvid

The port VLAN ID (PVID) is the VLAN to which incoming untagged and priority-tagged frames are classified on a general port. Use the `switchport general pvid` Interface Configuration (Ethernet, port-channel) mode command to configure the Port VLAN ID (PVID) of an interface when it is in general mode. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
switchport general pvid vlan-id
no switchport general pvid
```

**Parameters**

- **pvid vlan-id**—Specifies the Port VLAN ID (PVID).

**Default Configuration**

The default VLAN is the PVID.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Example**

**Example 1** - The following example configures port 2 as a general port and sets its PVID to 234.
Example 2 - Performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to general mode port 14
- Defines VID 100 as the PVID
- Reverts to the default PVID (VID=1)

```plaintext
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 234
```

Example 3 - Configures VLAN on port 14 as untagged on input and untagged on output:

```plaintext
switchxxxxxx(config)# interface gi1/1/14
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 2
switchxxxxxx(config-if)# switchport general allowed vlan add 2 untagged
```

Example 4 - Configures VLAN on port 21 as untagged on input and tagged on output:

```plaintext
switchxxxxxx(config)# interface gi1/1/21
switchxxxxxx(config-if)# switchport mode general
```
switchxxxxxx(config-if)#  switchport general pvid 2
switchxxxxxx(config-if)#  switchport general allowed vlan add 2  tagged
switchxxxxxx(config-if)#

Example 5 - Configures VLAN on port 14 as tagged on input and tagged on output:

switchxxxxxx(config)#  interface gi1/1/14
switchxxxxxx(config-if)#  switchport mode general
switchxxxxxx(config-if)#  switchport general allowed vlan add 2  tagged
switchxxxxxx(config-if)#

Example 6 - Configures VLAN on port 23 as tagged on input and untagged on output:

switchxxxxxx(config)#  interface gi1/1/23
switchxxxxxx(config-if)#  switchport mode general
switchxxxxxx(config-if)#  switchport general allowed vlan add 2  tagged
switchxxxxxx(config-if)#

34.17  switchport general ingress-filtering disable

Use the switchport general ingress-filtering disable Interface Configuration (Ethernet, port-channel) mode command to disable port ingress filtering (no packets are discarded at the ingress) on a general port. Use the no form of this command to restore the default configuration.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Parameters

N/A
Default Configuration
Ingress filtering is enabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example disables port ingress filtering on gi1/1/1.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

34.18 switchport general acceptable-frame-type

The `switchport general acceptable-frame-type` Interface Configuration mode command configures the types of packets (tagged/untagged) that are filtered (discarded) on the interface. Use the `no` form of this command to return ingress filtering to the default.

Syntax

```
switchport general acceptable-frame-type {tagged-only | untagged-only | all}
no switchport general acceptable-frame-type
```

Parameters

- `tagged-only`—Ignore (discard) untagged packets and priority-tagged packets.
- `untagged-only`—Ignore (discard) VLAN-tagged packets (not including priority-tagged packets)
- `all`—Do not discard packets untagged or priority-tagged packets.

Default Configuration
All frame types are accepted at ingress (all).
34.19 switchport customer vlan

When a port is in customer mode it is in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across a provider network. The switch is in QinQ mode when it has one or more customer ports.

Use the switchport customer vlan Interface Configuration mode command to set the port's VLAN when the interface is in customer mode (set by switchport mode). Use the no form of this command to restore the default configuration.

**Syntax**

```plaintext
switchport customer vlan vlan-id
no switchport customer vlan
```

**Parameters**

- `vlan vlan-id`—Specifies the customer VLAN.

**Default Configuration**

No VLAN is configured as customer.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode
Example

The following example defines gi1/1/5 as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

### 34.20 map protocol protocols-group

Forwarding of packets based on their protocol requires setting up groups of protocols and then mapping these groups to VLANs. Use the `map protocol protocols-group` VLAN Configuration mode command to map a protocol to a group of protocols. This protocol group can then be used in `switchport general map protocols-group vlan`. Use the `no` form of this command to delete a protocol from a group.

**Syntax**

```
map protocol protocol [encapsulation-value] protocols-group group
no map protocol protocol [encapsulation]
```

**Parameters**

- `protocol`—Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (range: 0x0600–0xFFFF)
- `encapsulation-value`—Specifies one of the following values: Ethernet, rfc1042, llcOther.
- `protocols-group group`—Specifies the group number of the group of protocols (range: 1–2147483647).

**Default Configuration**

The default encapsulation value is Ethernet.

**Command Mode**

VLAN Configuration mode
Virtual Local Area Network (VLAN) Commands

User Guidelines

The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ip
- arp
- ipv6
- ipx

Example

The following example maps the IP protocol to protocol group number 213.

```
switchxxxxx(config)# vlan database
switchxxxxx(config-vlan)# map protocol ip protocols-group 213
```

34.21 `switchport general map protocols-group vlan`

Use the `switchport general map protocols-group vlan` Interface Configuration (Ethernet, port-channel) mode command to forward packets based on their protocol, otherwise known as setting up a classifying rule. This command forwards packets arriving on an interface containing a specific protocol to a specific VLAN.

Use the no form of this command to stop forwarding packets based on their protocol.

Syntax

```
switchport general map protocols-group group vlan vlan-id
no switchport general map protocols-group group
```

Parameters

- `group`—Specifies the group number as defined in `map protocol protocols-group` (range: 1–65535).
- `vlan vlan-id`—Defines the VLAN ID in the classifying rule.
Default Configuration
N/A

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The VLAN classification rule priorities are:

2. MAC-based VLAN (best match among the rules)
3. Subnet-based VLAN (best match among the rules)
4. Protocol-based VLAN
5. PVID

Example
The following example forwards packets with protocols belong to protocol-group 1 to VLAN 8.

```
switchxxxxxx(config-if)# switchport general map protocols-group 1 vlan 8
```

### 34.22 show vlan protocols-groups

Use the `show vlan protocols-groups` EXEC mode command to display the protocols that belong to the defined protocols-groups.

Syntax

```
show vlan protocols-groups
```

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode
**Example**

The following example displays protocols-groups information.

```
switchxxxxxx# show vlan protocols-groups
```

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>Protocol</th>
<th>Group ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>0x800 (IP)</td>
<td>1</td>
</tr>
<tr>
<td>Ethernet</td>
<td>0x806 (ARP)</td>
<td>1</td>
</tr>
<tr>
<td>Ethernet</td>
<td>0x86dd (IPv6)</td>
<td>2</td>
</tr>
<tr>
<td>Ethernet</td>
<td>0x8898</td>
<td>3</td>
</tr>
</tbody>
</table>

**34.23 map mac macs-group**

Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Use the `map mac macs-group` VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses, which is then used in `switchport general map macs-group vlan`. Use the `no` form of this command to delete the mapping.

This command can only be used when the device is in Layer 2 mode.

**Syntax**

```
map mac mac-address [prefix-mask / host] macs-group group
no map mac mac-address [prefix-mask / host]
```

**Parameters**

- `mac mac-address`—Specifies the MAC address to be mapped to the group of MAC addresses.
- `prefix-mask`—Specifies the number of ones in the mask.
- `host`—Specifies that the mask is comprised of all 1s.
- `macs-group group`—Specifies the group number (range: 1–2147483647)

**Default Configuration**

N/A
Command Mode

VLAN Configuration mode

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

34.24 switchport general map macs-group vlan

After groups of MAC addresses have been created (see map mac macs-group), they can be mapped to specific VLANs.

Use the switchport general map macs-group vlan Interface Configuration (Ethernet, port-channel) mode command to set a MAC-based classification rule. Use the no form of this command to delete a classification rule.

Syntax

```
switchport general map macs-group group vlan vlan-id
no switchport general map macs-group group
```

Parameters

- **macs-group group**—Specifies the group number (range: 1–2147483647)
- **vlan vlan-id**— Defines the VLAN ID associated with the rule.

Default Configuration

N/A
Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules).
2. Subnet-based VLAN (Best match among the rules).
3. Protocol-based VLAN.
4. PVID.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gi1/1/11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

34.25 show vlan macs-groups

Use the `show vlan macs-groups` EXEC mode command to display the MAC addresses that belong to the defined MACs-groups.

Syntax

`show vlan macs-groups`

Parameters

N/A
### Default Configuration

N/A

### Command Mode

EXEC mode

### Example

The following example displays macs-groups information.

```bash
switchxxxx# show vlan macs-groups
```

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Mask</th>
<th>Group ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:12:34:56:78:90</td>
<td>20</td>
<td>22</td>
</tr>
<tr>
<td>00:60:70:4c:73:ff</td>
<td>40</td>
<td>1</td>
</tr>
</tbody>
</table>

### 34.26 switchport forbidden default-vlan

Use the `switchport forbidden default-vlan` Interface Configuration command to forbid a port from being added to the default VLAN. Use the no form of this command to revert to default.

#### Syntax

```
switchport forbidden default-vlan
no switchport forbidden default-vlan
```

#### Parameters

N/A

#### Default Configuration

Membership in the default VLAN is allowed.

#### Command Mode

Interface and Interface range configuration (Ethernet, port-channel)
User Guidelines

The command may be used at any time regardless of whether the port belongs to
the default VLAN.

The no command does not add the port to the default VLAN, it only defines an
interface as permitted to be a member of the default VLAN, and the port will be
added only when conditions are met.

Example

The following example forbids the port gi1 from being added to the default VLAN.

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# switchport forbidden default-vlan
```

34.27 switchport forbidden vlan

The switchport forbidden vlan Interface Configuration (Ethernet, port-channel)
mode command forbids adding or removing specific VLANs to or from a port.

Syntax

```
switchport forbidden vlan [add vlan-list | remove vlan-list]
```

Parameters

- **add vlan-list**—Specifies a list of VLAN IDs to add. Separate nonconsecutive
  VLAN IDs with a comma and no spaces; use a hyphen designate a range of
  IDs.

- **remove vlan-list**—Specifies a list of VLAN IDs to remove. Separate
  nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen
designate a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode
Example
The following example forbids adding VLAN IDs 234 to 256 to gi1/1/7.

```
switchxxxxxx(config)# interface gi1/1/7
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport forbidden vlan add 234-256
```

### 34.28 switchport default-vlan tagged

Use the `switchport default-vlan tagged` Interface Configuration command to configure the port as a tagged port in the default VLAN. Use the `no` form of the command to return the port to an untagged port.

**Syntax**

```
switchport default-vlan tagged
no switchport default-vlan tagged
```

**Parameters**

N/A

**Default Configuration**

If the port is a member in the default VLAN, by default, it is a member as an untagged port.

**Command Mode**

Interface configuration (Ethernet, port-channel)

**User Guidelines**

The command adds a port to the default VLAN as a tagged port.

The command is available only if the port mode is trunk or general.

When a trunk port is a member in the default VLAN as a tagged port then:

- The native VLAN cannot be the default VLAN
- The default of the native VLAN is 4095
Note: If the native VLAN of a port is the default VLAN when the port is added to the default VLAN as tagged, the native VLAN is set by the system to 4095.

When a general port is a member in the default VLAN as a tagged port then:

- The PVID can be the default VLAN.
- The default PVID is the default VLAN.

Note: The PVID is not changed when the port is added to the default VLAN as a tagged.

When executing the `switchport default-vlan tagged` command, the port is added (automatically by the system) to the default VLAN when the following conditions no longer exist:

- The port is a member in a LAG.
- The port is 802.1X unauthorized.
- An IP address is defined on the port.
- The port is a destination port of port mirroring.
- An IP address is defined on the default VLAN and the port is a PVE protected port.

The `no switchport default-vlan tagged` command removes the port from the default VLAN, and returns the default VLAN mode to untagged.

Note:

- If the native VLAN of a trunk port is 4095 when the port is removed from the default VLAN (as a tagged), the native VLAN is set by the system to the default VLAN.
- The PVID of a general port is not changed when the port is removed from the default VLAN (as a tagged). If the PVID is the default VLAN, the port is added by the system to the default VLAN as an untagged.

**Example**

The following example configures the port gi1/1/1 as a tagged port in the default VLAN.

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)#switchport default-vlan tagged
```
34.29  show interfaces switchport

Use the show interfaces switchport Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax

show interfaces switchport [interface-id]

Parameters

interface-id—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

Default Configuration

Displays information for all interfaces.

Command Mode

EXEC mode

Examples:

Example 1—The following example displays the command output for a trunk port:

```
switchxxxxxx# show interfaces switchport gi1/1/1
Port gi1/1/1:
Port Mode: Trunk
Ingress Filtering: Enabled
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN(NATIVE): 2
Gvrp Status: disabled
Protected: Enabled, Uplink is gi1/1/9.
802.1x state: single-host mode, authorized, PVID is changed to Radius assigned VLAN_ID
Port gi1/1/1 is member in:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>untagged</td>
<td>Default</td>
</tr>
</tbody>
</table>
```
Virtual Local Area Network (VLAN) Commands

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>tagged Dynamic</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>tagged Static</td>
</tr>
<tr>
<td>19</td>
<td>IPv6VLAN</td>
<td>untagged Static</td>
</tr>
<tr>
<td>72</td>
<td></td>
<td>untagged Static</td>
</tr>
<tr>
<td>120</td>
<td></td>
<td>untagged RADIUS Assigned VLAN</td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>Out</td>
</tr>
</tbody>
</table>

Classification rules:

Mac-based VLANs:

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Vlan ID</th>
</tr>
</thead>
</table>

Example 2—The following example displays the output for a general port:

```
switchxxxxxx# show interfaces switchport gi1/1/2
Port gi1/1/2:
Port mode: General
Ingress Filtering: Enabled
Acceptable Frame Type: admitAll
PVID: 4095 (discard vlan)
GVRP status: Enabled
Protected: Disabled
802.1x state: multi-sessions mode
Port gi1/1/2 is member in:
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>untagged</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>IP Telephony</td>
<td>tagged</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>Guest</td>
<td>untagged</td>
<td>Guest VLAN</td>
</tr>
<tr>
<td>120</td>
<td></td>
<td>untagged</td>
<td>RADIUS Assigned VLAN</td>
</tr>
<tr>
<td>200</td>
<td></td>
<td>untagged</td>
<td>RADIUS Assigned VLAN</td>
</tr>
</tbody>
</table>

Forbidden VLANS:
Example 3—The following example displays the command output for an access port:

```
switchxxxxxx# show interfaces switchport gi1/1/2
Port gi1/1/2:
Port Mode: Access
Ingress Filtering: Enabled
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN (NATIVE): 1
Gvrp Status: disabled
Protected: Disabled
802.1x state: multi-host mode, unauthorized, PVID is changed to the Guest VLAN_ID.
Port is member in:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Port Membership Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Untagged</td>
<td>System</td>
</tr>
<tr>
<td>102</td>
<td>Guest</td>
<td>Untagged</td>
<td>Guest VLAN</td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
</tr>
</thead>
</table>

Classification rules:

Mac based VLANs:

34.30 switchport access multicast-tv vlan

Use the `switchport access multicast-tv vlan` Interface Configuration (Ethernet, port-channel) mode command to enable receiving Multicast transmissions on an interface that is not the access port VLAN, while keeping the L2 segregation with subscribers on different access port VLANs. Use the `no` form of this command to disable receiving Multicast transmissions.
Virtual Local Area Network (VLAN) Commands

34

Syntax

switchport access multicast-tv vlan vlan-id
no switchport access multicast-tv vlan

Parameters

vlan-id—Specifies the Multicast TV VLAN ID.

Default Configuration

Receiving Multicast transmissions is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The user cannot transmit Multicast transmissions on the Multicast TV VLAN.

A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example

The following example enables gi1/1/5 to receive Multicast transmissions from VLAN 11.

switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11

34.31 switchport customer multicast-tv vlan

Use the switchport customer multicast-tv vlan Interface Configuration mode command to enable receiving Multicast transmissions from a VLAN that is not the customer port's VLAN, while keeping the L2 segregation with subscribers on different customer port VLANs.

Syntax

switchport customer multicast-tv vlan {add vlan-list | remove vlan-list}
Parameters
- **add vlan-list**—Specifies a list of Multicast TV VLANs to add to interface.
- **remove vlan-list**—Specifies a list of Multicast TV VLANs to remove from interface.

Default Configuration
The port is not a member in any Multicast TV VLAN.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The user cannot transmit Multicast transmissions on Multicast TV VLANs.
A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example
The following example enables gi1/1/5 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

### 34.32 show vlan multicast-tv

Use the **show vlan Multicast-tv** EXEC mode command to display the source and receiver ports of Multicast-TV VLAN. Source ports can transmit and receive traffic to/from the VLAN, while receiver ports can only receive traffic from the VLAN.

Syntax
```
show vlan Multicast-tv vlan vlan-id
```

Parameters
- **vlan-id**—Specifies the VLAN ID.
Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays information on the source and receiver ports of Multicast-TV VLAN 1000.

```
switchxxxxxx# show vlan multicast-tv vlan 1000
Source Ports     Receiver Ports
-----------------  -------------------
ge1/1/8, ge1/1/9  ge1/1/1-18
```

34.33 ip internal-usage-vlan

The system assigns a VLAN to every IP address. In rare cases, this might conflict with a user requirement for that VLAN. In this case, use the `ip internal-usage-vlan` Interface Configuration (Ethernet, port-channel) mode command to reserve a different VLAN as the internal usage VLAN of an interface. Use the `no` form of this command to restore the default configuration.

Syntax

```
ip internal-usage-vlan vlan-id
no ip internal-usage-vlan
```

Parameters

`vlan-id`—Specifies the internal usage VLAN ID.

Default Configuration

No VLAN is reserved as an internal usage VLAN by default (using this command).

Command Mode

Interface Configuration (Ethernet, port-channel) mode. It cannot be configured for a range of interfaces (range context).
User Guidelines

An internal usage VLAN is assigned by the system when an IP interface is defined on an Ethernet port or port-channel.

If an internal usage VLAN is not defined for a port, the software selects one of the unused VLANs.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following:

- Remove the IP address from the interface (this releases the internal usage VLAN).
- Recreate the VLAN on the required interface (now it will be assigned to the interface and not be used as an internal usage VLAN)
- Recreate the IP interface (another internal usage VLAN is assigned to this IP interface) or use this command to explicitly define the internal usage VLAN.

Example

The following example reserves unused VLAN 200 as the internal usage VLAN of gi1/1/3.

switchxxxxxx(config)# interface gi1/1/3
switchxxxxxx(config-if)# ip internal-usage-vlan 200

34.34 show vlan internal usage

Use the show vlan internal usage Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).

Syntax

show vlan internal usage

Parameters

N/A

Default Configuration

N/A
Command Mode

Privileged EXEC mode

Example

The following example displays the VLANs used internally by the device.

```
switchxxxxx# show vlan internal usage
Usage   VLAN   Reserved   IP address
-------- -------- ---------------
gi1/1/21  1007    No               Active
gi1/1/22  1008    Yes              Inactive
gi1/1/23  1009    Yes              Active
```

34.35 vlan prohibit-internal-usage

Use the `vlan prohibit-internal-usage` command in Global configuration mode to specify VLANs that cannot be used by the switch as internal VLANs.

Syntax

```
vlan prohibit-internal-usage none | {add | except | remove} vlan-list
```

Parameters

- **none**—The Prohibit Internal usage VLAN list is empty: any VLAN can be used by the switch as internal.
- **except**—The Prohibit Internal usage VLAN list includes all VLANs except the VLANs specified by the `vlan-list` argument: only the VLANs specified by the `vlan-list` argument can be used by the switch as internal.
- **add**—Adds the given VLANs to the Prohibit Internal usage VLAN list.
- **remove**—Remove the given VLANs from the Prohibit Internal usage VLAN list.
- **vlan-list**—List of VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. The VLAN ID that can be used is from 1 through 4094.
Default Configuration

The Prohibit Internal usage VLAN list is empty.

Command Mode

Global Configuration mode

User Guidelines

The switch requires an internal VLAN in the following cases:

- When an IP interface is defined directly on an Ethernet port or on a Port channel
- For each IPv6 tunnel, if IPv6 Routing is supported by the switch.

When a switch needs an internal VLAN it takes a free VLAN with the highest VLAN_ID.

Use the `vlan prohibit-internal-usage` command to define a list of VLANs that cannot be used as internal VLANs after reload.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following:

- Add the VLAN to the Prohibited User Reserved VLAN list.
- Copy the Running Configuration file to the Startup Configuration file
- Reload the switch
- Create the VLAN

Examples

Example 1—The following example specifies that VLANs 4010, 4012, and 4090-4094 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage add 4010,4012,4090-4094
```

Example 2—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage all
```
Example 3—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage 4000-4107
```
Voice VLAN Commands

35.1 voice vlan state

The voice vlan state Global Configuration mode command sets the type of voice VLAN that is functional on the device or disables voice VLAN entirely.

The no format of the command returns to the default.

Syntax

voice vlan state {{auto-enabled | auto-triggered} [ipv6] | oui-enabled | disabled}

no voice vlan state

Parameters

- oui-enabled—Voice VLAN is of type OUI.
- auto-enabled—Auto Voice VLAN is enabled.
- auto-triggered—Auto Voice VLAN on the switch is in standby and is put into operation when the switch detects a CDP device advertising a voice VLAN or if a voice VLAN ID is configured manually on the switch.
- disabled—Voice VLAN is disabled.
- ipv6—Auto VLAN is enabled on IPv6 mDNS.

Default Configuration

auto-triggered on ipv4

Command Mode

Global Configuration mode

User Guidelines

By factory default, CDP, LLDP, and LLDP-MED are enabled on the switch. In addition, manual Smartport mode and Basic QoS with trusted DSCP is enabled.

All ports are members of default VLAN 1, which is also the default Voice VLAN.
In addition, dynamic voice VLAN (auto-triggered) mode is the default mode of auto voice VLAN. In this mode, voice VLAN is enabled by a trigger (advertisement received by voice device attached to port).

If the administrative state is:

- **disabled** — The operational state is **disabled**.
- **oui-enabled** — The operational state is **oui-enabled**.
- **auto-enabled** — The operational state is **auto-enabled**.
- **auto-triggered** — The operational state is **auto-enabled** only if one of the following occurs:
  - A static local configured voice VLAN ID, CoS/802.1p, and/or DSCP that is not factory default is configured.
  - A CDP voice VLAN advertisement is received from a neighboring CDP device that is not a device of the same family as the current device.
  - A Voice Service Discovery Protocol (VSDP) message was received from a neighbor switch. VSDP is a Cisco Small Business proprietary protocol for SF and SG series managed switches.

In all other cases the operational state is **disabled**.

**Notes:**

- To change the administrative state from **oui-enabled** to **auto-enabled** (or auto-triggered), or vice versa, you must first set the administrative state to **disabled**.
- The administrative state cannot be set to **oui-enabled** if the Auto SmartPort administrative state is **enabled**.
- The administrative state cannot be set to **oui-enabled** if the voice VLAN is the default VLAN (VLAN 1). For **oui-enabled** mode, the voice VLAN cannot be 1.

**Examples:**

**Example 1** — The following example enables the OUI mode of Voice VLAN. The first try did not work - it was necessary to first disable voice VLAN.

```bash
switchxxxxxx(config)# voice vlan state oui-enabled
```

Disable the voice VLAN before changing the voice VLAN trigger.
Voice VLAN Commands

switchxxxxxx(config)#voice vlan state disabled
switchxxxxxx(config)#voice vlan state oui-enabled

Example 2 — The following example disables the Voice VLAN state. All auto Smartport configuration on ports are removed.

switchxxxxxx(config)#voice vlan state disabled
All interfaces with Auto Smartport dynamic type will be set to default.
Are you sure you want to continue? (Y/N) [Y] Y
switchxxxxxx(config)#30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 5
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 8
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 9
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 100

Example 3 — The following example sets the Voice VLAN state to auto-triggered. The VLANs are re-activated after auto SmartPort state is applied.

switchxxxxxx(config)#voice vlan state auto-triggered
switchxxxxxx(config)#30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 5
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 8
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 9
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 100

Example 4 — The following example sets the Voice VLAN state to auto-triggered on IPv6. The VLANs are re-activated after auto SmartPort state is applied.

switchxxxxxx(config)#voice vlan state auto-triggered ipv6
switchxxxxxx(config)#30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 5
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 8
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 9
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 100
Example 5 —The following example enables the OUI mode of Voice VLAN. The first try did not work - it was necessary to first disable voice VLAN.

```
switchxxxxxx(config)# voice vlan state oui-enabled
```
Disable the voice VLAN before changing the voice VLAN trigger.
```
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# voice vlan state oui-enabled
```

35.2 voice vlan refresh

The `voice vlan refresh` Global Configuration mode command restarts the Voice VLAN discovery process on all the Auto Voice VLAN-enabled switches in the VLAN by removing all externally learned voice VLAN attributes and resetting the voice VLAN to the default voice VLAN.

Syntax

```
voice vlan refresh
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# voice vlan refresh
switchxxxxxx(config)#

30-Apr-2011 02:01:02 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 100, VPT 5, DSCP 46 (Notification that Agreed Voice VLAN is updated)
(Auto Smartport configuration is changed)
30-Apr-2011 02:01:05 %LINK-W-Down: Vlan 50
```
30-Apr-2011 02:01:05 %LINK-W-Down: Vlan 100
30-Apr-2011 02:01:06 %LINK-I-Up: Vlan 50
30-Apr-2011 02:01:06 %LINK-I-Up: Vlan 100
switchxxxxxx#show voice vlan
Administrative Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 100
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)

(Following is the new active source)
Agreed Voice VLAN is received from switch b0:c6:9a:c1:da:00
Agreed Voice VLAN priority is 2 (active CDP device)
Agreed Voice VLAN-ID is 100
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Apr-30 02:01:02

35.3 voice vlan id

Use the voice vlan id Global Configuration mode command to statically configure the VLAN identifier of the voice VLAN. The no format of the command returns the voice VLAN to the default VLAN (1).

Syntax
voice vlan id vlan-id
no voice vlan id

Parameters
vlan id vlan-id—Specifies the voice VLAN (range 1-4094).

Default Configuration
VLAN ID 1.
Voice VLAN Commands

Command Mode
Global Configuration mode

User Guidelines
If the Voice VLAN does not exist, it is created automatically. It will not be removed automatically by the no version of this command.

Example
The following example enables VLAN 35 as the voice VLAN on the device.

```
switchxxxxxx(config)# voice vlan id 35
```

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N)[Y] Y

30-Apr-2011 00:19:36 %VLAN-I-VoiceVlanCreated: Voice Vlan ID 104 was created.

```
30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 5, DSCP 46
```

35.4 voice vlan vpt

Use the `voice vlan vpt` Global Configuration mode command to specify a value of VPT (802.1p VLAN priority tag) that will be advertised by LLDP in the Network Policy TLV. The no format of the command returns the value to the default.

Syntax

```
voice vlan vpt vpt-value
no voice vlan vpt
```

Parameters

- `vpt vpt-value`—The VPT value to be advertised (range 0-7).

Default Configuration
5
**Command Mode**

Global Configuration mode

**Example**

The following example sets 7 as the voice VLAN VPT. A notification that the new settings are different than the old ones is displayed.

```
switchxxxxxx(config)# voice vlan vpt 7
```

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N)[Y] Y

30-Apr-2011 00:24:52 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 5, DSCP 46

```
switchxxxxxx(config)#
```

30-Apr-2011 00:25:07 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 46

**35.5 voice vlan dscp**

Use the `voice vlan dscp` Global Configuration mode command to specify a value of DSCP that will be advertised by LLDP in the Network Policy TLV. The `no` format of the command returns the value to the default.

**Syntax**

```
voice vlan dscp dscp-value
no voice vlan dscp
```

**Parameters**

- `dscp dscp-value`—The DSCP value (range 0-63).

**Default Configuration**

46
Command Mode

Global Configuration mode

Example

The following example sets 63 as the voice VLAN DSCP.

```
switchxxxxxx(config)# voice vlan dscp 63
```

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N) [Y] Y

30-Apr-2011 00:31:07 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 7, DSCP 46

```
switchxxxxxx(config)#30-Apr-2011 00:31:22 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 63
```

35.6 voice vlan oui-table

Use the voice vlan oui-table Global Configuration mode command to configure the voice OUI table. Use the no form of this command to restore the default configuration.

Syntax

```
voice vlan oui-table {add mac-address-prefix | remove mac-address-prefix} [text]
```

no voice vlan oui-table

Parameters

- **add** `mac-address-prefix`—Adds the specified MAC address prefix to the voice VLAN OUI table (length: 3 bytes).

- **remove** `mac-address-prefix`—Removes the specified MAC prefix address from the voice VLAN OUI table (length: 3 bytes).

- **text**—Adds the specified text as a description of the specified MAC address to the voice VLAN OUI table (length: 1–32 characters).
Default Configuration

The default voice VLAN OUI table is:

<table>
<thead>
<tr>
<th>OUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:e0:bb</td>
<td>3COM Phone</td>
</tr>
<tr>
<td>00:03:6b</td>
<td>Cisco Phone</td>
</tr>
<tr>
<td>00:e0:75</td>
<td>Veritel Polycom Phone</td>
</tr>
<tr>
<td>00:d0:1e</td>
<td>Pingtel Phone</td>
</tr>
<tr>
<td>00:01:e3</td>
<td>Siemens AG Phone</td>
</tr>
<tr>
<td>00:60:b9</td>
<td>NEC/Philips Phone</td>
</tr>
<tr>
<td>00:0fe2</td>
<td>Huawei-3COM Phone</td>
</tr>
<tr>
<td>00:09:e2</td>
<td>Avaya Phone</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration mode

User Guidelines

The classification of a packet from VoIP equipment/phones is based on the packet's OUI in the source MAC address. OUIs are globally assigned (administered) by the IEEE.

In MAC addresses, the first three bytes contain a manufacturer ID (Organizationally Unique Identifiers (OUI)) and the last three bytes contain a unique station ID.

Since the number of IP phone manufacturers that dominates the market is limited and well known, the known OUI values are configured by default and OUIs can be added/removed by the user when required.

Example

The following example adds an entry to the voice VLAN OUI table.

```
switchxxxxxx(config)# voice vlan oui-table add 00:AA:BB description experimental
```
35.7 voice vlan cos mode

Use the voice vlan cos mode Interface Configuration mode command to select the OUI voice VLAN Class of Service (CoS) mode. Use the no form of this command to return to the default.

Syntax

voice vlan cos mode {src / all}
no voice vlan cos mode

Parameters

- src—QoS attributes are applied to packets with OUIs in the source MAC address. See the User Guidelines of voice vlan oui-table.
- all—QoS attributes are applied to packets that are classified to the Voice VLAN.

Default Configuration

The default mode is src.

Command Mode

Global Configuration mode

Example

The following example applies QoS attributes to voice packets.

switchxxxxxx(config)# voice vlan cos mode all

35.8 voice vlan cos

Use the voice vlan cos Global Configuration mode command to set the OUI Voice VLAN Class of Service (CoS). Use the no form of this command to restore the default configuration.

Syntax

voice vlan cos cos [remark]
no voice vlan cos
Parameters

- **cos cos**—Specifies the voice VLAN Class of Service value. (Range: 0–7)
- **remark**—Specifies that the L2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 5.
The L2 user priority is not remarked by default.

Command Mode

Global Configuration mode

Example

The following example sets the OUI voice VLAN CoS to 7 and does not do remarking.

```
switchxxxxxx(config)# voice vlan cos 7
```

### 35.9 voice vlan aging-timeout

Use the **voice vlan aging-timeout** Global Configuration mode command to set the OUI Voice VLAN aging timeout interval. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
voice vlan aging-timeout minutes
no voice vlan aging-timeout
```

**Parameters**

- **aging-timeout minutes**—Specifies the voice VLAN aging timeout interval in minutes. (Range: 1–43200).

**Default Configuration**

1440 minutes
**35Voice VLAN Commands**

**Command Mode**

Global Configuration mode

**Example**

The following example sets the OUI Voice VLAN aging timeout interval to 12 hours.

```
switchxxxxxx(config)# voice vlan aging-timeout 720
```

---

**35.10 voice vlan enable**

Use the `voice vlan enable` Interface Configuration (Ethernet, Port-channel) mode command to enable OUI voice VLAN configuration on an interface. Use the `no` form of this command to disable OUI voice VLAN configuration on an interface.

**Syntax**

- `voice vlan enable`
- `no voice vlan enable`

**Default Configuration**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

This command is applicable only if the voice VLAN state is globally configured as OUI voice VLAN (using `voice vlan state`).

The port is added to the voice VLAN if a packet with a source MAC address OUI address (defined by `voice vlan oui-table`) is trapped on the port. Note: The packet VLAN ID does not have to be the voice VLAN, it can be any VLAN.

The port joins the voice VLAN as a tagged port.

If the time since the last MAC address with a source MAC address OUI address was received on the interface exceeds the timeout limit (configured by `voice vlan aging-timeout`), the interface is removed from the voice VLAN.
Example

The following example enables OUI voice VLAN configuration on gi1/1/2.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# voice vlan enable
```

### 35.11 show voice vlan

Use the `show voice vlan` EXEC mode command to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI.

**Syntax**

```
show voice vlan [type [oui | auto]] [interface-id | detailed]
```

**Parameters**

- **type oui**—Common and OUI-voice-VLAN specific parameters are displayed.
- **type auto**—Common and Auto Voice VLAN-specific parameters are displayed.
- **interface-id**—Specifies an Ethernet port ID. Relevant only for the OUI type.
- **detailed**—Displays information for non-present ports in addition to present ports. Only valid when type is oui.

**Default Configuration**

If the **type** parameter is omitted the current Voice VLAN type is used.

If the **interface-id** parameter is omitted then information about all interfaces is displayed.

All ports are displayed. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**User Guidelines**

Using this command without parameters displays the current voice VLAN type parameters and local and agreed voice VLAN settings.
Using this command with the **type** parameter displays the voice VLAN parameters relevant to the type selected. The the local and agreed voice VLAN settings are displayed only if this is the current voice VLAN state.

The interface-id parameter is relevant only for the OUI VLAN type.

**Examples:**

The following examples display the output of this command in various configurations.

**Example 1**—Displays the **auto** voice VLAN parameters (this is independent of the voice VLAN state actually enabled).

```bash
switch>show voice vlan type auto
switchxxxxxx#show voice vlan type auto
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is 0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
switchxxxxxx#
```

**Example 2**—Displays the current voice VLAN parameters when the voice VLAN state is auto-enabled.

```bash
switch>show voice vlan
Administrative Voice VLAN state is auto-enabled on IPv4
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is 0 (active static source)
```
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 16:48:13
switchxxxxxx#

Example 3—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered but voice VLAN has not been triggered.

switch>show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is disabled
VSDP Authentication is disabled

Example 4—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered and it has been triggered.

switchxxxxxx(config)#voice vlan state auto-triggered
switchxxxxxx(config)#voice vlan state auto-triggered
operational voice vlan state is auto
admin state is auto triggered
switchxxxxxx#show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
**Example 5**—Displays the current voice VLAN parameters when both auto voice VLAN and OUI are disabled.

```
switch>show voice vlan
switchxxxxxx#show voice vlan
Administrative Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Aging timeout: 1440 minutes
```

**Example 6**—Displays the voice VLAN parameters when the voice VLAN operational state is OUI.

```
switch>show voice vlan
Administrative Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:E0:BB</td>
<td>3COM</td>
<td></td>
</tr>
<tr>
<td>00:03:6B</td>
<td>Cisco</td>
<td></td>
</tr>
<tr>
<td>00:E0:75</td>
<td>Veritel</td>
<td></td>
</tr>
<tr>
<td>00:D0:1E</td>
<td>Pingtel</td>
<td></td>
</tr>
<tr>
<td>00:01:E3</td>
<td>Simens</td>
<td></td>
</tr>
<tr>
<td>00:60:B9</td>
<td>NEC/Philips</td>
<td></td>
</tr>
</tbody>
</table>
```
35.12 show voice vlan local

The show voice vlan local EXEC mode command displays information about the auto voice VLAN local configuration, including the best local voice VLAN.

Syntax

show voice vlan local

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Examples:

Example 1—A CDP device is connected to an interface and a conflict is detected:

30-Apr-2011 00:39:24 %VLAN-W-ConflictingCDPDetected: conflict detected between operational VLAN and new CDP device 00:1e:13:73:3d:62 on interface gi7. Platform TLV is -4FXO-K9, Voice VLAN-ID is 100...

switchxxxxxx#show voice vlan local
Administrate Voice VLAN state is auto-triggered on IPv6
Operational Voice VLAN state is auto-enabled
VSDP Authentication is enabled, key string name is alpha
The character '*; marks the best local Voice VLAN

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>46</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>*104</td>
<td>7</td>
<td>63</td>
<td>static</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
<td>CDP</td>
<td>00:1e:13:73:3d:62</td>
<td>gi1/1/7</td>
</tr>
</tbody>
</table>

Example 2—Displays the local voice VLAN configuration when the voice VLAN state is auto-triggered.

switchxxxxxx#show voice vlan local

Administrate Voice VLAN state is auto-triggered on IPv4
Operational Voice VLAN state is auto-enabled

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>46</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>*100</td>
<td></td>
<td></td>
<td>CDP</td>
<td>00:23:56:1a:dc:68</td>
<td>gi1/1/11</td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
<td>CDP</td>
<td>00:44:55:44:55:4d</td>
<td>gi1/1/11</td>
</tr>
</tbody>
</table>

The character "*" marks the best local voice VLAN.

Example 3—Displays the local voice VLAN configuration when the voice VLAN state is OUI.

switchxxxxxx#show voice vlan local

Administrate Voice VLAN state is auto-OUI
Operational Voice VLAN state is OUI
The character '*; marks the best local Voice VLAN

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>*10</td>
<td>1</td>
<td>27</td>
<td>static</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>-----</td>
<td>---</td>
<td>----</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>10</td>
<td>CDP</td>
<td>00:00:12:ea:87:dc</td>
<td>gi1/1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>CDP</td>
<td>00:00:aa:aa:89:dc</td>
<td>pol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SSD Commands

36.1 ssd config

Use `ssd config` in Global Configuration to enter the Secure Sensitive Data (SSD) command mode. In this command mode, an administrator can configure how the sensitive data on the device, such as keys and passwords, is to be protected.

**Syntax**

`ssd config`

**Command Mode**

Global Configuration mode

**User Guidelines**

Only users with sufficient permission can use this command, which edits and displays the SSD configuration. See `ssd rule` for a description of these permissions.

**Example**

```
switchxxxxx(config)# ssd config
switchxxxxx(ssd-config)#
```

36.2 passphrase

Use `passphrase` in SSD Command mode to change the passphrase in the system. A device protects its sensitive data by encrypting them using the key generated from the passphrase.

Use the `no passphrase` to reset the passphrase to the default passphrase.

**Syntax**

`passphrase {passphrase}`

`encrypted passphrase {encrypted-passphrase}`

`no passphrase`
Parameters

- **passphrase**-New system passphrase.
- **encrypted-passphrase**-The passphrase in its encrypted form.

Default Usage

If this command is not entered, the default passphrase is used.

Command Mode

SSD Command Mode

User Guidelines

To use this command, enter passphrase and Enter, a confirmation message is displayed and the user must confirm the intention to change the passphrase. Then the passphrase can be entered (see example).

Encrypted passphrase is allowed only in the SSD Control Block of a source file that is being copied to the startup configuration file (user cannot manually enter this command).

When generating a passphrase, the user must use 4 different character classes (similar to strong password/passwords complexity). These can be: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.

Example

The following example defines a decrypted passphrase.

```
switchxxxxxx(ssd-config)# passphrase
This operation will change the system SSD passphrase. Are you sure? (Y/N)[N] Y
Please enter SSD passphrase:**********
Please reenter SSD passphrase:**********
```

36.3 ssd rule

Use **ssd rule** in SSD Command mode to configure an SSD rule. A device grants read permission of sensitive data to user based on the SSD rules. A user that is granted Both or Plaintext read permission is also granted permission to enter SSD Command Mode.

Use **no ssd rule** to delete user-defined rules and restore default rules.
**SSD Commands**

**Syntax**

```
[encrypted] SSD rule {all | level-15 | default-user | user user-name}
  {secure | insecure | secure-xml-snmp | insecure-xml-snmp}
  permission {encrypted-only | plaintext-only | both | exclude}
  default-read {encrypted | plaintext | exclude}
no ssd rule {all | level-15 | default-user | user user-name}
  {secure | insecure | secure-xml-snmp | insecure-xml-snmp}
```

**Command Mode**

SSD command mode.

**Default Rules**

The device has the following factory default rules:

<table>
<thead>
<tr>
<th>Rule Key</th>
<th>Rule Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Channel</td>
</tr>
<tr>
<td>level-15</td>
<td>secure-xml-snmp</td>
</tr>
<tr>
<td>level-15</td>
<td>secure</td>
</tr>
<tr>
<td>level-15</td>
<td>insecure</td>
</tr>
<tr>
<td>all</td>
<td>insecure-xml-snmp</td>
</tr>
<tr>
<td>all</td>
<td>secure</td>
</tr>
<tr>
<td>all</td>
<td>insecure</td>
</tr>
</tbody>
</table>

**User Guidelines**

Use **no ssd rule** to delete a user-defined rule or to restore the default of a modified default rule.

Use **no ssd rule** (without parameters) to remove all SSD rules and restore the default SSD rules. A confirmation message will be displayed asking permission to do this.

To delete specific rules (applicable for the user defined), provide parameters specifying the user and security of the channel.

**encrypted SSD rule** is used to copy an SSD rule from one device to another in a secure manner.
You can modify but cannot delete the default SSD rules.

The following is the order in which SSD rules are applied:

- The SSD rules for specified users.
- The SSD rule for the default-user (cisco).
- The SSD rules for level-15 users.
  - The remaining SSD rules for all.

The user can enter the commands in any order. The ordering is done implicitly by the device.

**Examples**

**Example 1** - The following example modifies a rule.

```bash
switchxxxxxx(ssd-config)#ssd rule level-15 secure permission encrypted-only
default-read encrypted
```

**Example 2** - The following example adds a rule.

```bash
switchxxxxxx(ssd-config)#ssd rule user james secure permission both default-read encrypted
```

**Example 3** - The following example adds a rule as encrypted format.

```bash
switchxxxxxx(ssd-config)#encrypted ssd rule iurwe874jho32iu9ufjo32i83232fdefsd
```

**Example 4** - The following example deletes a default rule.

```bash
switchxxxxxx(ssd-config)#no ssd rule all secure
```

**Example 5** - The following example deletes a user-defined rule.

```bash
switchxxxxxx(ssd-config)#no ssd rule user james secure
```

**Example 6** - The following example deletes all rules.

```bash
switchxxxxxx(ssd-config)#no ssd rule
```

This operation will delete all user-defined rules and retrieve the default rules instead.

Are you sure (Y/N): N
36.4  show SSD

Use `show ssd rules` in SSD Command mode to present the current SSD rules; the rules will be displayed as plaintext.

**Syntax**

`show SSD [rules | brief]`

**Parameters**

- **rules** - Display only the SSD rules.
- **brief** - Display the encrypted passphrase, File Passphrase Control and File Integrity attributes.

**Command Mode**

SSD Command mode

Privileged EXEC mode

**Default Configuration**

Display all SDD information.

**Examples**

**Example 1** - The following example displays all SSD information.

```
switchxxxxxx (ssd-config)#show ssd
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled

SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled

User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
Specific    admin11       secure            Both        Encrypted   User-Define
Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
Level-15    secure-xml-snmp  Plaintext-Only   Plaintext  Default
```
Example 2 - The following example displays the SSD rules.

```
switchxxxxxx(ssd-config)#show ssd rules

<table>
<thead>
<tr>
<th>User Type</th>
<th>User Name</th>
<th>Channel</th>
<th>Read Permission</th>
<th>Default Read</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific</td>
<td>admin11</td>
<td>secure</td>
<td>Both</td>
<td>Encrypted</td>
<td>User-Define</td>
</tr>
<tr>
<td>Specific</td>
<td>admin2</td>
<td>secure</td>
<td>Encrypted-Only</td>
<td>Encrypted</td>
<td>User-Define</td>
</tr>
<tr>
<td>Level-15</td>
<td></td>
<td>secure-xml-snmp</td>
<td>Plaintext-Only</td>
<td>Plaintext</td>
<td>*Default</td>
</tr>
<tr>
<td>Level-15</td>
<td></td>
<td>secure</td>
<td>Both</td>
<td>Encrypted</td>
<td>Default</td>
</tr>
<tr>
<td>Level-15</td>
<td></td>
<td>insecure</td>
<td>Both</td>
<td>Encrypted</td>
<td>Default</td>
</tr>
<tr>
<td>All</td>
<td></td>
<td>secure</td>
<td>Encrypted-Only</td>
<td>Encrypted</td>
<td>Default</td>
</tr>
<tr>
<td>All</td>
<td></td>
<td>insecure</td>
<td>Encrypted-Only</td>
<td>Encrypted</td>
<td>Default</td>
</tr>
<tr>
<td>All</td>
<td></td>
<td>insecure-xml-snmp</td>
<td>Plaintext-Only</td>
<td>Plaintext</td>
<td>*Default</td>
</tr>
</tbody>
</table>
```

* Modified default entry

Example 3 - The following example displays the SSD attributes.

```
switchxxxxxx(ssd-config)#show ssd brief

SSD current parameters:
Local Passphrase:    Default
File Passphrase Control: Unrestricted
File Integrity Control: Disabled

SSD parameters after reset:
Local Passphrase:    Default
File Passphrase Control: Unrestricted
File Integrity Control: Disabled
```

36.5 `ssd session read`

Use `ssd session read` in Global Configuration mode to override the current SSD default read of the current session.
SSD Commands

36

36.6  show ssd session

Use **show ssd session** in Exec mode to view the SSD read permission and default read mode of the user of the current session.

Syntax

`show ssd session`
Command Mode
EXEC mode.

Default
N/A

Examples
switchxxxxxx# show ssd session
User Name/Level: James / Level 15
User Read Permission: Both
Current Session Read mode: Plaintext

36.7 ssd file passphrase control
Use ssd file passphrase control in SSD Command mode to provide an additional level of protection when copying configuration files to the startup configuration file. The passphrase in a configuration file is always encrypted with the default passphrase key.

Syntax
ssd file passphrase control {restricted | unrestricted}
no ssd file passphrase control

Parameters

- **Restricted** - In this mode, a device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. The mode should be used when a user does not want to expose the passphrase in a configuration file.

- **Unrestricted** - In this mode, a device will include its passphrase when creating a configuration file. This allows any devices accepting the configuration file to learn the passphrase from the file.

Default
The default is unrestricted.
**Command Mode**

SSD Command mode.

**User Guidelines**

To revert to the default state, use the `no ssd file passphrase control` command.

Note that after a device is reset to the factory default, its local passphrase is set to the default passphrase. As a result, the device will not be able to decrypted sensitive data encrypted with a user-defined passphrase key in its own configuration files until the device is manually configured with the user-passphrase again or the files are created in unrestricted mode.

If a user-defined passphrase in Unrestricted mode are configured, it is highly recommended to enable SSD File Integrity Control. Enabling SSD File Integrity Control protects configuration files from tampering.

**Examples**

```plaintext
console(ssd-config)# ssd file passphrase control restricted
console(ssd-config)# no ssd file passphrase control
```

### 36.8 ssd file integrity control

Use `ssd file integrity control` command in SSD Command Mode to instruct the device to protect newly-generated configuration files that contain encrypted sensitive data from tampering.

Use `no ssd file integrity control` to disable Integrity Control.

**Syntax**

`ssd file integrity control enabled`

`no ssd file integrity control`

**Parameters**

- `enabled` - Enable file integrity control to protect newly-generated configuration files from tampering.

**Default**

The default file input control is `disable`. 
Command Mode

SSD Command Mode.

User Guidelines

A user can protect a configuration file from being tampered by creating the file with File Integrity Control enabled. It is recommended that File Integrity Control be enabled when a device uses a user-defined passphrase with Unrestricted Configuration File Passphrase Control.

A device determines whether the integrity of a configuration file is protected by examining the File Integrity Control command in the file. If a file is integrity-protected, but a device finds the integrity of the file is not intact, the device rejects the file. Otherwise, the file is accepted for further processing.

Examples

switchxxxxxx(ssd-config)# ssd file integrity control enabled

When File Integrity is enabled, an internal digest command is added to the end of the entire configuration file. This is used in downloading the configuration file to the startup configuration.

config-file-digest 0AC78001122334400AC780011223344
37.1 macro auto (Global)

The **macro auto** Global Configuration mode command sets the Auto Smartports administrative global state. The **no** format of the command returns to the default.

**Syntax**

```plaintext
macro auto {enabled | disabled | controlled}
no macro auto
```

**Parameters**

- **enabled**—Auto Smartport administrative global and operational states are enabled.
- **disabled**—Auto Smartport administrative global and operational states are disabled.
- **controlled**—Auto Smartport administrative global and operational states are enabled when Auto Voice VLAN is in operation.

**Default Configuration**

Administrative state is **controlled**.

**Command Mode**

Global Configuration mode

**User Guidelines**

Regardless of the status of Auto Smartport, you can always manually apply a Smartport macro to its associated Smartport type. A Smartport macro is either a built-in macro or a user-defined macro. You can define and apply a macro using the CLI commands presented in the Macro Commands section.

If the Auto Smartport Administrative state is controlled, the Auto Smartport Operational state is managed by the Voice VLAN manager and is set as follows:

- Auto Smartport Operational state is disabled when the OUI Voice VLAN is enabled.
Auto Smartport Operational state is enabled when the Auto Voice VLAN is enabled.

A user cannot enable Auto Smartport globally if the OUI Voice VLAN is enabled.

Example

This example shows an attempt to enable the Auto Smartport feature globally in the controlled mode. This is not possible because the OUI voice feature is enabled. The voice VLAN state is then disabled, after which Auto Smartports can be enabled. The appropriate VLANs are automatically enabled because the ports are configured for Auto Smartports on these VLANs.

```
switchxxxxxx(config)# macro auto controlled
switchxxxxxx(config)# macro auto enabled
Auto smartports cannot be enabled because OUI voice is enabled.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# macro auto enabled
switchxxxxxx(config)#10-Apr-2011 16:11:31 %LINK-I-Up: Vlan 20
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 5
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 6
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 7
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 8
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 9
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 10
```

37.2 macro auto smartport (Interface)

The `macro auto smartport` Interface Configuration mode command enables the Auto Smartport feature on a given interface. The `no` format of the command disables the feature on the interface.

**Syntax**

`macro auto smartport`

`no macro auto smartport`
Parameters
N/A

Default Configuration
Enabled.

Command Mode
Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines
This command is effective only when Auto Smartport is globally enabled.

Example
Enables the Auto Smartport feature on port 1:

```
switchxxxxx(conf)#interface gi1/1/1
switchxxxxx(conf-if)# macro auto smartport
```

37.3  macro auto trunk refresh

The `macro auto trunk refresh` Global Configuration command reapplies the Smartport macro on a specific interface, or to all the interfaces with the specified Smartport type.

Syntax
`macro auto trunk refresh [smartport-type] [interface-id]`

Parameters
- `smartport-type`—Smartport type (switch, router, wireless access point (ap))
- `interface-id`—Interface Identifier (port or port channel).

Default Configuration
See User Guidelines.
**Command Mode**
Global Configuration mode

**User Guidelines**
The macro auto smartport command becomes effective only when the Auto Smartport is globally enabled.

If both smartport-type and interface-id are defined, the attached Smartport macro is executed on the interface if it has the given Smartport type.

If only smartport-type is defined, the attached Smartport macro is executed on all interfaces having the given Smartport type.

If only interface-id is defined then the corresponding attached Smartport macro is executed if the interface has one of the following Smartport types: switch, router or wireless access point (ap).

If a Smartport macro contains configuration commands that are no longer current on one or more interfaces, you can update their configuration by reapplying the Smartport macro on the interfaces.

**Example**
Adds the ports of Smartport type switch to all existing VLANs by running the associated Smartport macros.

```
switchxxxxxx(conf)#macro auto trunk refresh switch
```

### 37.4 macro auto resume

The macro auto resume Interface Configuration mode command changes the Smartport type from unknown to default and resumes the Smartport feature on a given interface (but does not reapply the Smartport macro; this is done by macro auto trunk refresh).

**Syntax**
macro auto resume

**Parameters**
N/A
Default Configuration
N/A

Command Mode
Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines
When a Smartport macro fails at an interface, the Smartport type of the interface becomes Unknown. You must diagnose the reason for the failure on the interface and/or Smartport macro, and correct the error. Before you or Auto Smartport are allowed to reapply the desired Smartport macro, you must reset the interface using the macro auto resume command, which changes the Smartport type of the interface to Default. Then you can run macro auto trunk refresh.

Example
Changes the Smartport type from unknown to default and resumes the Smartport feature on port 1.

```
switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if)#macro auto resume
```

37.5 macro auto persistent

The macro auto persistent Interface Configuration mode command sets the interface as a Smartport persistent interface. The no format of the command returns it to default.

Syntax
macro auto persistent
no macro auto persistent

Parameters
N/A

Default Configuration
Not persistent.
Command Mode

Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines

A Smartport’s persistent interface retains its dynamic configuration in the following cases: link down/up, the attaching device ages out, and reboot. Note that for persistence and the Smartport configuration to be effective across reboot, the Running Configuration file must be saved to the Startup Configuration file.

Example

The example establishes two port ranges and makes one persistent and the other not.

```
switchxxxxxx(config)#interface range gi1/1/1-2
switchxxxxxx(config-if-range)#macro auto persistent
switchxxxxxx(config-if-range)#exit
switchxxxxxx(config)#interface range gi1/1/3-4
switchxxxxxx(config-if-range)#no macro auto persistent
```

37.6  macro auto smartport type

The `macro auto smartport type` Interface Configuration mode command manually (statically) assigns a Smartport type to an interface. The `no` format of the command removes the manually-configured type and returns it to default.

Syntax

```
macro auto smartport type smartport-type [parameter-name value [parameter-name value [parameter-name value]]]
```

Parameters

- `smartport-type` — Smartport type.
- `parameter-name value` — Specifies the parameter name and its value (Range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).
Default Configuration

*parameter-name value*—Parameter default value. For instance, if the parameter is the voice VLAN, the default value is the default voice VLAN.

Command Mode

Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines

A static type set by the command cannot be changed by a dynamic type.

Example

This example shows an attempt to set the Smartport type of port 1 to printer (statically). The macro fails at line 10. The `show parser macro name` command is run to display the contents of the macro printer in order to see which line failed.

```
switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if)#macro auto smartport type printer
30-May-2011 15:02:45 %AUTOSMARTPORT-E-FAILEDMACRO: Macro printer for auto smartport type Printer on interface gi1 failed at command number 10
switchxxxxxx(conf-if)#exit
switchxxxxxx(conf-if)#do show parser macro name printer
Macro name : printer
Macro type : default interface
   1. #macro description printer
   2. #macro keywords $native_vlan
   3. 
   4. #macro key description: $native_vlan: The untag VLAN which will be configured on the port
   5. #Default Values are
   6. #$native_vlan = Default VLAN
   7. 
   8. #the port type cannot be detected automatically
   9. 
```
10. switchport mode access
11. switchport access vlan $native_vlan
12. #
13. #single host
14. port security max 1
15. port security mode max-addresses
16. port security discard trap 60
17. #
18. smartport storm-control broadcast level 10
19. smartport storm-control include-multicast
20. smartport storm-control broadcast enable

switch030008(config)#

### 37.7 macro auto processing cdp

The **macro auto processing cdp** Global Configuration mode command enables using CDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the CDP capabilities advertised by the attaching device(s).

The **no** format of the command disables the feature.

**Syntax**

`macro auto processing cdp`

`no macro auto processing cdp`

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Global Configuration
Example

To enable CDP globally:

```
switchxxxxx(conf)#macro auto processing cdp
```

### 37.8 macro auto processing lldp

The **macro auto processing lldp** Global Configuration mode command enables using the LLDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the LLDP capabilities advertised by the attaching device(s).

The **no** format of the command disables the feature.

**Syntax**

```
macro auto processing lldp
no macro auto processing lldp
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Global Configuration

**Example**

To enable LLDP globally:

```
switchxxxxx(conf)#macro auto processing lldp
```
37.9 macro auto processing type

The macro auto processing type Global Configuration mode command enables or disables automatic detection of devices of given type. The no format of the command returns to the default.

Syntax

macro auto processing type smartport-type {enabled | disabled}

no macro auto processing type smartport-type

Parameters

smartport-type—Smartport type (range: host, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

Default Configuration

By default, auto detection of ip_phone, ip_phone_desktop, switch, and wireless access point (ap) is enabled.

Command Mode

Global Configuration

Example

In this example, automatic detection of wireless access points (ap) is enabled.

switchxxxxxx(config)#macro auto processing type ?
host set type to host
ip_phone set type to ip_phone
ip_phone_desktop set type to ip_phone_desktop
switch set type to switch
router set type to router
ap set type to access point
switchxxxxxx(config)#macro auto processing type ap enabled
37.10  macro auto user smartport macro

The macro auto user smartport macro Global Configuration mode command links user-defined Smartport macros to a Smartport type. This is done by replacing the link to the built-in macro with the link to the user-defined macro. The no format of the command returns the link to the default built-in Smartport macro.

Syntax

macro auto user smartport macro smartport-type user-defined-macro-name
[parameter-name value [parameter-name value [parameter-name value]]]

no macro auto user smartport macro smartport-type

Parameters

- **smartport macro smartport-type**—Smartport type (range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

- **smartport macro user-defined-macro-name**—Specifies the user-defined macro name that replaces the built-in Smartport macro.

- **parameter-name value**—Specifies the parameter name and its value in the user-defined macro.

Default Configuration

**parameter-name value**—Parameter’s default value. For instance, if the parameter is the native VLAN, the default value is the default native VLAN.

Command Mode

Global Configuration

User Guidelines

The scope of each parameter is the macro in which it is defined, with the exception of the parameter $voice_vlan, which is a global parameter and its value is specified by the switch and cannot be defined in a macro.

The macros must be defined before linking them in this command.

Smartport macros must be disconnected from the Smartport type before removing them (using the no version of this command).

To associate a Smartport type with a user-defined macros, you must have defined a pair of macros: one to apply the configuration, and the other (anti macro) to
remove the configuration. The macros are paired by their name. The name of the
anti macro is the concatenation of no_ with the name of the corresponding macro.
Please refer to the Macro Command section for details about defining macro.

Example

To link the user-defined macro: my_ip_phone_desktop to the Smartport type:
ip_phone_desktop and provide values for its two parameters:

```
switchxxxxxx(conf)#macro auto user smartport macro ip_phone_desktop
my_ip_phone_desktop $p1 1 $p2 2
```

37.11 macro auto built-in parameters

The **macro auto built-in parameters** Global Configuration mode command
replaces the default Auto Smartport values of built-in Smartport macros. The **no**
format of the command returns to the default values.

**Syntax**

```
macro auto built-in parameters smartport-type [parameter-name value
[parameter-name value [parameter-name value]]]
no macro auto built-in parameters smartport-type
```

**Parameters**

- **smartport-type**—Smartport type (range: printer, desktop, guest, server,
host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless
access point (ap)).

- **parameter-name value**—Specifies the parameter name and its value. These
are the parameters of the built-in or user-defined macro defined in macro
auto user smartport macro.

**Default Configuration**

The default value of parameter $native_vlan of the built-in Smartport macros is 1.

For other parameters, the default value is the parameter’s default value. For
instance, if the parameter is the native VLAN, the default value is the default native
VLAN.
Command Mode
Global Configuration

User Guidelines

By default, each Smartport type is associated with a pair of built-in macros: a macro that applies the configuration and the anti macro (no macro) to remove the configuration. The Smartport types are the same as the name of the corresponding built-in Smartport macros, with the anti macro prefixed with no_.

The value of the parameter $voice_vlan cannot be changed by this command.

Example

To change the parameters of a built-in macro:

```
switchxxxxxx(conf)#macro auto built-in parameters switch $native_vlan 2
```

37.12 show macro auto processing

The show macro auto processing EXEC mode command displays information about which protocols (CDP/LLDP) are enabled and which device types can be detected automatically.

Syntax

```
show macro auto processing
```

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC

Example

```
switchxxxxxx#show macro auto processing
```
37.13 show macro auto smart-macros

The `show macro auto smart-macros` EXEC mode command displays the name of Smartport macros, their type (built-in or user-defined) and their parameters. This information is displayed for all Smartport types or for the specified one.

Syntax

```
show macro auto smart-macros [smartport-type]
```

Parameters

smartport-type—Smartport type (range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

Default Configuration

N/A

Command Mode

EXEC

Example

```
switchxxxxxx#show macro auto smart-macros
SG300-52-R#show macro auto smart-macros
SmartPort type : printer
Parameters     : $native_vlan=1
SmartPort Macro: printer (Built-In)
```
SmartPort type: desktop
Parameters: $max_hosts=10 $native_vlan=1
SmartPort Macro: desktop (Built-In)

SmartPort type: guest
Parameters: $native_vlan=1
SmartPort Macro: guest (Built-In)

SmartPort type: server
Parameters: $max_hosts=10 $native_vlan=1
SmartPort Macro: server (Built-In)

SmartPort type: host
Parameters: $max_hosts=10 $native_vlan=1
SmartPort Macro: host (Built-In)

SmartPort type: ip-camera
Parameters: $native_vlan=1
SmartPort Macro: ip_camera (Built-In)

SmartPort type: ip-phone
Parameters: $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone (Built-In)

SmartPort type: ip-phone-desktop
Parameters: $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone_desktop (Built-In)

SmartPort type: switch
Parameters: $native_vlan=1 $voice_vlan=1
SmartPort Macro: switch (Built-In)

SmartPort type: router
Parameters: $native_vlan=1 $voice_vlan=1
SmartPort Macro: router (Built-In)

SmartPort type: ap
Parameters: $native_vlan=1 $voice_vlan=1
SmartPort Macro: ap (Built-In)

SG300-52-R#
### 37.14 show macro auto ports

The `show macro auto ports` EXEC mode command displays information about all Smartport ports or a specific one. If a macro was run on the port and it failed, the type of the port is displayed as Unknown.

**Syntax**

```
show macro auto ports [interface-id | detailed]
```

**Parameters**

- `interface-id`—Interface Identifier (Ethernet interface, port channel)
- `detailed`—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Information about all ports is displayed.

**Command Mode**

EXEC

**Examples**

**Example 1**—Note that Smartport on switch and phone types was configured automatically. Smartport on routers was configured statically.

```
switchxxxxxx# show macro auto ports
```

```
Smartport is enabled
Administrative Globally Auto Smartport is enabled
Operational Globally Auto Smartport is enabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto Smartport</th>
<th>Persistent</th>
<th>Smartport Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>disabled</td>
<td>enabled</td>
<td>switch</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>enabled</td>
<td>enabled</td>
<td>default</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Enabled</th>
<th>Disabled</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/3</td>
<td>enabled</td>
<td>disabled</td>
<td>phone</td>
</tr>
<tr>
<td>gi1/1/4</td>
<td>enabled</td>
<td>enabled</td>
<td>router (static)</td>
</tr>
<tr>
<td>gi1/1/5</td>
<td>enabled</td>
<td>enabled</td>
<td>switch</td>
</tr>
<tr>
<td>gi1/1/6</td>
<td>enabled</td>
<td>enabled</td>
<td>unknown</td>
</tr>
</tbody>
</table>

**Example 2—Disabling auto SmartPort on gi2:**

```
switchxxxxxx(config-if)#interface gi1/2
switchxxxxxx(config-if)#no macro auto smartport
switchxxxxxx(config-if)#end
switchxxxxxx#show macro auto ports gi1/2
```

SmartPort is Enabled
Administrative Globally Auto SmartPort is controlled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is disabled on gi2
Persistent state is not-persistent
Interface type is default
No macro has been activated

**Example 3—Enabling auto SmartPort on gi1:**

```
switchxxxxxx(config-if)#interface gi1/1
switchxxxxxx(config-if)#macro auto smartport
switchxxxxxx(config-if)#end
switchxxxxxx#show macro auto ports gi1/1
```

SmartPort is Enabled
Administrative Globally Auto SmartPort is enabled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is enabled on gi1/1
Persistent state is persistent
Interface type is switch
Last activated macro is switch
37.15 smartport switchport trunk allowed vlan

The `smartport switchport trunk allowed vlan` Interface Configuration (Ethernet, port-channel) mode command adds/removes VLANs to/from a trunk port.

**Syntax**

```plaintext
smartport switchport trunk allowed vlan {add \[vlan-list / all\] | remove \[vlan-list / all\]}
```

**Parameters**

- **add vlan-list**—Specifies a list of VLAN IDs to add to interface. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **add all**—Add all VLANs to interface.
- **remove vlan-list**—Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **remove all**—Remove all VLANs from interface.

**Default Configuration**

N/A

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

This command is an extension of the `switchport trunk allowed vlan` command. Unlike the `switchport trunk allowed vlan` command, the `vlan-list` parameter of this command may include the voice VLAN (when it is the default VLAN). If the default VLAN is the voice VLAN, the following occurs:

- **add all** — Adds the interface to the default VLAN as an egress tagged port.
- **remove all** — Removes the interface from the default VLAN.

**Example**

To add port 1 to VLANs 1-5:

```
switchxxxxxx(conf)#interface gi1/1/1
```
37.16  **smartport switchport trunk native vlan**

Use the **smartport switchport trunk native vlan** Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN when the interface is in trunk mode. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
smartport switchport trunk native vlan native-vlan-id
```

**Parameters**

- **native-vlan-id**—Specifies the native VLAN ID.

**Default Configuration**

VLAN 1

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

This command is an extension of the **switchport trunk native vlan** CLI command. Unlike the **switchport trunk native vlan** CLI command, this command may also be applied to the default VLAN when the interface belongs to the default VLAN as egress tagged port.

**Example**

Define the native VLAN when port 1 is in trunk mode:

```
switchxxxxxx(conf-if)#smartport switchport trunk allowed vlan add 1-5
```

```
switchxxxxxx(conf-if)#smartport switchport trunk native vlan 1
```

37.17  **smartport storm-control broadcast enable**

Use the **smartport storm-control broadcast enable** Interface Configuration (Ethernet, port-channel) mode command to enable storm control on a Smartport port. Use the **no** form of this command to disable storm control.
Syntax

smartport storm-control broadcast enable

Parameters

N/A

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if)#smartport storm-control broadcast enable

37.18  smartport storm-control broadcast level

Use the `smartport storm-control broadcast level` Interface Configuration (Ethernet, port-channel) mode command to control the amount of Broadcast traffic allowed on an interface.

Syntax

smartport storm-control broadcast level {level | kbps kbps}

no smartport storm-control broadcast level

Parameters

- **level**—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1 -100)
- **kbps**—Maximum of kilobits per second of broadcast traffic on a port. (Range 70–10000000)

Default Configuration

- **level**—10%
- **kbps**—10% of port speed in Kbps
Command Mode

Interface Configuration (Ethernet, port-channel) mode

Examples

Example 1 - Set the maximum number of kilobits per second of Broadcast traffic on port 1 to 10000.

```
switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if)#smartport storm-control broadcast level kpbs 10000
```

Example 2 - Set the maximum percentage of kilobits per second of Broadcast traffic on port 1 to 30%.

```
switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if)#smartport storm-control broadcast level 30
```

37.19 smartport storm-control include-multicast

Use the `smartport storm-control include-multicast` Interface Configuration mode command to count Multicast packets in a Broadcast storm control. Use the `no` form of this command to disable counting of Multicast packets in the Broadcast storm control.

Syntax

```
smartport storm-control include-multicast [unknown-unicast]
no smartport storm-control include-multicast
```

Parameters

- `unknown-unicast`—Specifies also the count of unknown Unicast packets.

Default Configuration

Disabled

Command Mode

Interface Configuration mode (Ethernet)
Example

```
switchxxxxx(config)# interface gi1/1
switchxxxxx(config-if)# smartport storm-control include-multicast
```
CDP Commands

38.1 cdp run

The cdp run Global Configuration mode command enables CDP globally. The no format of this command disabled CDP globally.

Syntax

cdp run

no cdp run

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

CDP is a link layer protocols for directly-connected CDP/LLDP-capable devices to advertise themselves and their capabilities. In deployments where the CDP/LLDP capable devices are not directly connected and are separated with CDP/LLDP incapable devices, the CDP/LLDP capable devices may be able to receive the advertisement from other device(s) only if the CDP/LLDP incapable devices flood the CDP/LLDP packets they receives. If the CDP/LLDP incapable devices perform VLAN-aware flooding, then CDP/LLDP capable devices can hear each other only if they are in the same VLAN. It should be noted that a CDP/LLDP capable device may receive advertisement from more than one device if the CDP/LLDP incapable devices flood the CDP/LLDP packets.

To learn and advertise CDP information, it must be globally enabled (it is so by default) and also enabled on interfaces (also by default).

Example
38.2 cdp enable

The `cdp enable` Interface Configuration mode command enables CDP on interface. The `no` format of the CLI command disables CDP on an interface.

**Syntax**

```
cdp enable
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Ethernet Interface

**User Guidelines**

For CDP to be enabled on an interface, it must first be enabled globally using `cdp run`.

**Example**

```
switchxxxxxx(conf) cdp run
switchxxxxxx(conf) interface gi1
switchxxxxxx(conf-if) cdp enable
```

38.3 cdp pdu

Use the `cdp pdu` Global Configuration mode command when CDP is not enabled globally. It specifies CDP packets handling when CDP is globally disabled. The `no` format of this command returns to default.

**Syntax**

```
cdp pdu [filtering | bridging | flooding]
```
no cdp pdu

Parameters

- **filtering**—Specify that when CDP is globally disabled, CDP packets are filtered (deleted).
- **bridging**—Specify that when CDP is globally disabled, CDP packets are bridged as regular data packets (forwarded based on VLAN).
- **flooding**—Specify that when CDP is globally disabled, CDP packets are flooded to all the ports in the product that are in STP forwarding state, ignoring the VLAN filtering rules.

Default Configuration

bridging

Command Mode

Global Configuration mode

User Guidelines

When CDP is globally enabled, CDP packets are filtered (discarded) on CDP-disabled ports.

In the flooding mode, VLAN filtering rules are not applied, but STP rules are applied. In case of MSTP, the CDP packets are classified to instance 0.

Example

switchxxxxxx(conf) cdp run

switchxxxxxx(conf) cdp pdu flooding

38.4 cdp advertise-v2

The `cdp advertise-v2` Global Configuration mode command specifies version 2 of transmitted CDP packets. The `no` format of this command specifies version 1.

Syntax

cdp advertise-v2

no cdp advertise-v2
Parameters
N/A

Default Configuration
Version 2.

Command Mode
Global Configuration mode

Example

switchxxxxxx(conf) cdp run
switchxxxxxx(conf) cdp advertise-v2

38.5 cdp appliance-tlv enable

The cdp appliance-tlv enable Global Configuration mode command enables sending of the Appliance TLV. The no format of this command disables the sending of the Appliance TLV.

Syntax

cdp appliance-tlv enable
no cdp appliance-tlv enable

Parameters
N/A

Default Configuration
Enabled

Command Mode
Global Configuration mode

User Guidelines
This MIB specifies the Voice Vlan ID (VVID) to which this port belongs:
• 0—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with value of 0. VoIP and related packets are expected to be sent and received with VLAN-ID=0 and an 802.1p priority.

• 1..4094—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with N. VoIP and related packets are expected to be sent and received with VLAN-ID=N and an 802.1p priority.

• 4095—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with value of 4095. VoIP and related packets are expected to be sent and received untagged without an 802.1p priority.

• 4096—The CDP packets transmitting through this port do not include Appliance VLAN-ID TLV; or, if the VVID is not supported on the port, this MIB object will not be configurable and will return 4096.

Example

switchxxxxxx(conf) cdp appliance-tlv enable

38.6 cdp mandatory-tlvs validation

Use the cdp mandatory-tlvs validation Global Configuration mode command to validate that all mandatory (according to the CDP protocol) TLVs are present in received CDP frames. The no format of this command disables the validation.

If the mandatory TLVs are not included in the packet, it is deleted.

Syntax

cdp mandatory-tlvs validation

no cdp mandatory-tlvs validation

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode
Example

This example turns off mandatory TLV validation:

```
switchxxxxxx(conf) no cdp mandatory-tlvs validation
```

### 38.7 cdp source-interface

The `cdp source-interface` Global Configuration mode command specifies the CDP source port used for source IP address selection. The `no` format of this command deletes the source interface.

**Syntax**

```
cdp source-interface interface-id
no cdp source-interface
```

**Parameters**

`interface-id`—Source port used for Source IP address selection.

**Default Configuration**

No CDP source interface is specified.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `cdp source-interface` command to specify an interface whose minimal IP address will be advertised in the TVL instead of the minimal IP address of the outgoing interface.

**Example**

```
switchxxxxxx(conf) cdp source-interface gi1/1/1
```
38.8  cdp log mismatch duplex

Use the `cdp log mismatch duplex` Global and Interface Configuration mode command to enable validating that the duplex status of a port received in a CDP packet matches the port's actual configuration. If not, a SYSLOG duplex mismatch message is generated. The `no` format of the CLI command disables the generation of the SYSLOG messages.

**Syntax**

cdp log mismatch duplex

no cdp log mismatch duplex

**Parameters**

N/A

**Default Configuration**

The switch reports duplex mismatches from all ports.

**Command Mode**

Global Configuration mode

Ethernet Interface

**Example**

```
switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if) cdp log mismatch duplex
```

38.9  cdp log mismatch voip

Use the `cdp log mismatch voip` Global and Interface Configuration mode command to enable validating that the VoIP status of the port received in a CDP packet matches its actual configuration. If not, a SYSLOG message is generated by CDP. The `no` format of the CLI command disables the generation of the SYSLOG messages.

**Syntax**

cdp log mismatch voip
no cdp log mismatch voip

Parameters
N/A

Default Configuration
The switch reports VoIP mismatches from all ports.

Command Mode
Global Configuration mode
Interface Configuration mode (Ethernet)

Example

switchxxxxxx(conf) interface gi1/1/1
switchxxxxxx(conf-if) cdp log mismatch voip

38.10 cdp log mismatch native

Use the cdp log mismatch native Global and Interface Configuration mode command to enable validating that the native VLAN received in a CDP packet matches the actual native VLAN of the port. If not, a SYSLOG native mismatch message is generated. The no format of the CLI command disables the generation of the SYSLOG messages.

Syntax

cdp log mismatch native

no cdp log mismatch native

Parameters
N/A

Default Configuration
The switch reports native VLAN mismatches from all ports.
**Command Mode**

Global Configuration mode

Interface Configuration mode (Ethernet)

**Example**

```
switchxxxxxx(conf)
  interface gi1/1/1
switchxxxxxx(conf-if)
  cdp log mismatch native
```

### 38.11 cdp device-id format

The `cdp device-id format` Global Configuration mode command specifies the format of the Device-ID TLV. The `no` format of this command returns to default.

**Syntax**

```
cdp device-id format {mac | serial-number | hostname}
no cdp device-id format
```

**Parameters**

- `mac`—Specifies that the Device-ID TLV contains the device's MAC address.
- `serial-number`—Specifies that Device-ID TLV contains the device's hardware serial number.
- `hostname`—Specifies that Device-ID TLV contains the device's hostname.

**Default Configuration**

MAC address is selected by default.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(conf) cdp device-id format serial-number
```
38.12  cdp timer
The cdp timer Global Configuration mode command specifies how often CDP packets are transmitted. The no format of this command returns to default.

Syntax

```plaintext
 cdp timer seconds
 no cdp timer
```

Parameters

- **seconds**—Value of the Transmission Timer in seconds. Range: 5-254 seconds.

Default Configuration

60 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(conf) cdp timer 100
```

38.13  cdp holdtime
The cdp holdtime Global Configuration mode command specifies a value of the Time-to-Live field into sent CDP messages. The no format of this command returns to default.

Syntax

```plaintext
 cdp holdtime seconds
 no cdp holdtime
```

Parameters

- **seconds**—Value of the Time-to-Live field in seconds. The value should be greater than the value of the Transmission Timer.
Parameters range
seconds—10 - 255.

Default Configuration
180 seconds.

Command Mode
Global Configuration mode

Example

switchxxxxx(conf) cdp holdtime 100

38.14 clear cdp counters

The clear cdp counters Global Configuration mode command resets the CDP traffic counters to 0.

Syntax

clear cdp counters [global] interface-id

Parameters

- **global**—Clear only the global counters.
- **interface-id**—Specifies the interface identifier of the counters that should be cleared.

Command Mode

Global Configuration mode

User Guidelines

Use the clear cdp counters global to clear only the global counters. Use the cdp counters interface-id command to clear the counters of the given interface. Use the command cdp counters without parameters to clear all the counters.

Example

switchxxxxx(config) clear cdp counters global
### 38.15 clear cdp table

The **clear cdp table** Global Configuration mode command deletes the CDP Cache tables.

**Syntax**

```
clear cdp table
```

**Parameters**

N/A

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(conf) clear cdp table
```

### 38.16 show cdp

The **show cdp** Privileged EXEC mode command displays the interval between advertisements, the number of seconds the advertisements are valid and version of the advertisements.

**Syntax**

```
show cdp
```

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxx>show cdp
Global CDP information:
  cdp is globally enabled
  cdp log duplex mismatch is globally enabled
```
cdp log voice VLAN mismatch is globally enabled
cdp log native VLAN mismatch is globally disabled
Mandatory TLVs are
  Device-ID TLV (0x0001)
  Address TLV (0x0002)
  Port-ID TLV (0x0003)
  Capabilities TLV (0x0004)
  Version TLV (0x0005)
  Platform TLV (0x0006)
Sending CDPv2 advertisements is enabled
Sending Appliance TLV is enabled
Device ID format is Serial Number
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds

38.17 show cdp entry

The `show cdp entry` Privileged EXEC mode command displays information about specific neighbor. Display can be limited to protocol or version information.

Syntax

```
show cdp entry {* | device-name}[protocol | version]
```

Parameters

- `*`—Specifies all neighbors
- `device-name`—Specifies the name of the neighbor.
- `protocol`—Limits the display to information about the protocols enabled on neighbors.
- `version`—Limits the display to information about the version of software running on the neighbors.

Default Configuration

Version

Command Mode

Privileged EXEC mode
Example

switchxxxxxx#show cdp entry device.cisco.com
Device ID: device.cisco.com
Advertisement version: 2
Entry address(es):
   IP address: 192.168.68.18
   CLNS address: 490001.1111.1111.1111.00
   DECnet address: 10.1
Platform: cisco 4500,  Capabilities: Router
Interface: gi1/1/1,  Port ID (outgoing port): Ethernet0
Holdtime: 125 sec
Version:
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M), Version 11.1(10.4), MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by dschwart

switchxxxxxx#show cdp entry device.cisco.com protocol
Protocol information for device.cisco.com:
   IP address: 192.168.68.18
   CLNS address: 490001.1111.1111.1111.00
   DECnet address: 10.1

switchxxxxxx#show cdp entry device.cisco.com version
Version information for device.cisco.com:
   Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M), Version 11.1(10.4), MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by dschwart

38.18  show cdp interface

The show cdp interface Privileged EXEC mode command displays information about ports on which CDP is enabled.
**Syntax**

`show cdp interface interface-id`

**Parameters**

`interface-id`—Port ID.

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxxx#show cdp interface gi1/1/1
CDP is globally enabled
CDP log duplex mismatch
  Globally is enabled
  Per interface is enabled
CDP log voice VLAN mismatch
  Globally is enabled
  Per interface is enabled
CDP log native VLAN mismatch
  Globally is disabled
  Per interface is enabled
gi1 is Down, CDP is enabled
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
```

### 38.19 show cdp neighbors

The `show cdp neighbors` Privileged EXEC mode command displays information about neighbors kept in the main or secondary cache.

**Syntax**

`show cdp neighbors [interface-id] [detail | secondary]`

**Parameters**

- `interface-id`—Displays the neighbors attached to this port.
- **detail**—Displays detailed information about a neighbor (or neighbors) from the main cache including network address, enabled protocols, hold time, and software version.

- **secondary**—Displays information about neighbors from the secondary cache.

**Default Configuration**

If an interface ID is not specified, the command displays information for the neighbors of all ports.

If **detail** or **secondary** are not specified, the default is **secondary**.

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxxxx#show cdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone,

M - Remotely-Managed Device, C - CAST Phone Port, W - Two-Port MAC Relay
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone
M - Remotely-Managed Device, C - CAST Phone Port,
W - Two-Port MAC Relay

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Interface</th>
<th>Adv Ver</th>
<th>Adv Time</th>
<th>Capabilities</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTK-SW-A-86.marvel</td>
<td>gi48</td>
<td>2</td>
<td>147</td>
<td>S I</td>
<td>cisco GigabitEthercom</td>
<td>GigabitEthernet3/39</td>
</tr>
<tr>
<td>ESW-520-8P</td>
<td>gi48</td>
<td>2</td>
<td>153</td>
<td>S I M</td>
<td>ESW-520-8P</td>
<td>g1</td>
</tr>
<tr>
<td>ESW-540-8P</td>
<td>gi48</td>
<td>2</td>
<td>146</td>
<td>S I M</td>
<td>ESW-540-8P</td>
<td>g9</td>
</tr>
<tr>
<td>003106131611</td>
<td>gi48</td>
<td>2</td>
<td>143</td>
<td>S I</td>
<td>Cisco SG500-28P (PID:SG500-28P)</td>
<td>fa2/2/1</td>
</tr>
<tr>
<td>001828100211</td>
<td>gi48</td>
<td>2</td>
<td>173</td>
<td>S I</td>
<td>Cisco SF 200-48P (PID:SLM248P T)-VSD</td>
<td>fa20</td>
</tr>
<tr>
<td>c47d4fed9302</td>
<td>gi48</td>
<td>2</td>
<td>137</td>
<td>S I</td>
<td>Cisco SF 200-48P</td>
<td>fa12</td>
</tr>
</tbody>
</table>

```
switchxxxxxxx#show cdp neighbors detail
-------------------------
Device ID: lab-7206
Advertisement version: 2
Entry address(es):
    IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): gi1/1/0
Time To Live : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Duplex: half
```
Device ID: lab-as5300-1
Entry address(es):
    IP address: 172.19.169.87
Platform: cisco AS5300, Capabilities: Router
Device ID: SEP000427D400ED
Advertisement version: 2
Entry address(es):
    IP address: 1.6.1.81
Platform: Cisco IP Phone 7940, Capabilities: Host
Interface: gi1/1/1, Port ID (outgoing port): Port 1
Time To Live: 150 sec
Version :
P00303020204
Duplex: full
sysName: a-switch
Power drawn: 6.300 Watts

switchxxxxxx#show cdp neighbors secondary
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>Mac Address</th>
<th>TimeToLive</th>
<th>Capability</th>
<th>VLAN-ID</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>00:00:01:23a:86:9c</td>
<td>157</td>
<td>R,S</td>
<td>10</td>
<td>206VXRYC</td>
</tr>
<tr>
<td>gi1/1/1</td>
<td>00:00:05:53a:86:9c</td>
<td>163</td>
<td>R,S</td>
<td>10</td>
<td>ABCD-VSD</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>00:00:01:23b:86:9c</td>
<td>140</td>
<td>R</td>
<td></td>
<td>QACSZ</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>00:00:ab:c2a:86:9c</td>
<td>132</td>
<td>T</td>
<td></td>
<td>CAT3000</td>
</tr>
</tbody>
</table>

Field Definitions:

- **Advertisement version**—The version of CDP being used for CDP advertisements.
- **Capabilities**—The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.

- **COS for Untrusted Ports**—The COS value with which all packets received on an untrusted port should be marked by a simple switching device which cannot itself classify individual packets.

- **Device ID**—The name of the neighbor device and either the MAC address or the serial number of this device.

- **Duplex**—The duplex state of connection between the current device and the neighbor device.

- **Entry address(es)**—A list of network addresses of neighbor devices.

- **Extended Trust**—The Extended Trust.

- **External Port-ID**—Identifies the physical connector port on which the CDP packet is transmitted. It is used in devices, such as those with optical ports, in which signals from multiple hardware interfaces are multiplexed through a single physical port. It contains the name of the external physical port through which the multiplexed signal is transmitted.

- **Interface**—The protocol and port number of the port on the current device.

- **IP Network Prefix**—It is used by On Demand Routing (ODR). When transmitted by a hub router, it is a default route (an IP address). When transmitted by a stub router, it is a list of network prefixes of stub networks to which the sending stub router can forward IP packets.

- **Management Address**—When present, it contains a list of all the addresses at which the device will accept SNMP messages, including those it will only accept when received on interface(s) other than the one over which the CDP packet is being sent.

- **MTU**—The MTU of the interface via which the CDP packet is sent.

- **Native VLAN**—The ID number of the VLAN on the neighbor device.

- **Physical Location**—A character string indicating the physical location of a connector which is on, or physically connected to, the interface over which the CDP packet containing this TLV is sent.

- **Platform**—The product name and number of the neighbor device. In the case of the Secondary Cache only the 8 last characters of the value are printed.
- **Power Available**—Every switch interface transmits information in the Power Available TLV, which permits a device which needs power to negotiate and select an appropriate power setting. The Power Available TLV includes four fields.

- **Power Consumption**—The maximum amount of power, in milliwatts, expected to be obtained and consumed from the interface over which the CDP packet is sent.

- **Power Drawn**—The maximum requested power.

  Note: For IP Phones the value shown is the maximum requested power (6.3 Watts). This value can be different than the actual power supplied by the routing device (generally 5 watts; shown using the show power command).

- **Protocol-Hello**—Specifies that a particular protocol has asked CDP to piggyback its "hello" messages within transmitted CDP packets.

- **Remote Port_ID**—Identifies the port the CDP packet is sent on.

- **sysName**—An ASCII string containing the same value as the sending device's sysName MIB object.

- **sysObjectID**—The OBJECT-IDENTIFIER value of the sending device's sysObjectID MIB object.

- **Time To Live**—The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.

- **Version**—The software version running on the neighbor device.

- **Voice VLAN-ID**—The Voice VLAN-ID.

- **VTP Management Domain**—A string that is the name of the collective group of VLANs associated with the neighbor device.

### 38.20 show cdp tlv

The `show cdp tlv` Privileged EXEC mode command displays information about TLVs sent by CDP on all ports or on a specific port.

**Syntax**

```
show cdp tlv [interface-id]
```
Parameters

interface-id—Port ID.

Default Configuration

TLVs for all ports.

Command Mode

Privileged EXEC mode

User Guidelines

You can use the `show cdp tlv` command to verify the TLVs configured to be sent in CDP packets. The `show cdp tlv` command displays information for a single port if specified or for all ports if not specified. Information for a port is displayed if only CDP is really running on the port, i.e. CDP is enabled globally and on the port, which is UP.

Examples:

Example 1 - In this example, CDP is disabled and no information is displayed.

```
switchxxxxxx#show cdp tlv
cdp globally is disabled
```

Example 2 - In this example, CDP is globally enabled but disabled on the port and no information is displayed.

```
switchxxxxxx#show cdp tlv gi1/1/2
cdp globally is enabled
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone, M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/1/2
CDP is disabled on gi1/1/2
```
Example 3 - In this example, CDP is globally enabled and enabled on the port, but the port is down and no information is displayed.

```
switchxxxxxx# show cdp tlv interface gi1/1/2
cdp globally is enabled
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone, M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/1/3
CDP is enabled on gi1/1/3
Ethernet gi1/1/3 is down
```

Example 4 - In this example, CDP is globally enabled and enabled on the port, which is up and information is displayed.

```
switchxxxxxx# show cdp tlv interface gi1/1/1
cdp globally is enabled
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone, M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/1/1
CDP is enabled
Ethernet gi1/1/1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4: 1.2.2.2 IPv6:
Port_ID TLV: gi1/1/1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
```
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
    Available-Power is 10;
    Management-Power-Level is 0xFFFFFFFF

**Example 5** - In this example, CDP is globally enabled, and no ports are specified, so information is displayed for all ports on which CDP is enabled who are up.

    switchxxxxxx#show cdp tlv interface
    cdp globally is enabled

    Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
    S - Switch, H - Host, I - IGMP, r - Repeater,
    P - VoIP Phone, M - Remotely-Managed Device,
    C - CAST Phone Port, W - Two-Port MAC Relay
    Interface TLV: gi1/1/1
    CDP is enabled
    Ethernet gi1/1/1 is up,
    Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
    Address TLV: IPv4: 1.2.2.2 IPv6:
    Port_ID TLV: gi1/1/s1
    Capabilities: S, I
    Version TLV: 1 and 2
    Platform TLV: VSD Ardd
    Native VLAN TLV: 1
    Full/Half Duplex TLV: full-duplex
    Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
    COS for Untrusted Ports TLV: 1
    sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
Available-Power is 10;
Management-Power-Level is 0xFFFFFFFF

Interface TLV: gi1/1/2
CDP is disabled on gi1/1/2

Interface TLV: gi1/1/3
CDP is enabled on gi1/1/3
Ethernet gi1/1/3 is down

### 38.21 show cdp traffic

The `show cdp traffic` Privileged EXEC mode command displays the CDP counters, including the number of packets sent and received and checksum errors.

**Syntax**

```
show cdp traffic [global | interface-id]
```

**Parameters**

- `global`—Display only the global counters
- `interface-id`—Port for which counters should be displayed.

**Default Configuration**

If `interface-id` is not specified, global counters are displayed for all ports on which CDP is enabled and who are up.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use the `show cdp traffic global` to display only the global counters. Use the `show cdp traffic interface-id` command to display the counters of the given port. Use the command `show cdp traffic` without parameters to display all the counters.

**Example**

```
switchxxxxxx#show cdp traffic
```
CDP Commands

CDP Global counters:

- Total packets output: 81684, Input: 81790
- Hdr syntax: 0, Chksum error: 0, Encaps: 0
- No memory: 0, Invalid packet: 0
- CDP version 1 advertisements output: 100, Input 0
- CDP version 2 advertisements output: 81784, Input 0

```
gil/1/1
  Total packets output: 81684, Input: 81790
  Hdr syntax: 0, Chksum error: 0, Encaps: 0
  No memory: 0, Invalid packet: 0
  CDP version 1 advertisements output: 100, Input 0
  CDP version 2 advertisements output: 81784, Input 0
```

```
gil/1/2
  Total packets output: 81684, Input: 81790
  Hdr syntax: 0, Chksum error: 0, Encaps: 0
  No memory: 0, Invalid packet: 0
  CDP version 1 advertisements output: 100, Input 0
  CDP version 2 advertisements output: 81784, Input 0
```

Field Definition:

- **Total packets output**—The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.

- **Input**—The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.

- **Hdr syntax**—The number of CDP advertisements with bad headers, received by the local device.

- **Chksum error**—The number of times the checksum (verifying) operation failed on incoming CDP advertisements.

- **No memory**—The number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table.
when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.

- **Invalid**—The number of invalid CDP advertisements received.

- **CDP version 1 advertisements output**—The number of CDP Version 1 advertisements sent by the local device.

- **CDP version 1 advertisements Input**—The number of CDP Version 1 advertisements received by the local device.

- **CDP version 2 advertisements output**—The number of CDP Version 2 advertisements sent by the local device.

- **CDP version 2 advertisements Input**—The number of CDP Version 2 advertisements received by the local device.
# Link Layer Discovery Protocol (LLDP) Commands

## 39.1 `lldp run`

Use the `lldp run` Global Configuration mode command to enable LLDP. To disable LLDP, use the `no` form of this command.

**Syntax**

```
lldp run
no lldp run
```

**Parameters**

N/A.

**Default Configuration**

Enabled

**Command Mode**

Global Configuration mode

**Example**

```bash
switchxxxxxx(config)# lldp run
```

## 39.2 `lldp transmit`

Use the `lldp transmit` Interface Configuration mode command to enable transmitting LLDP on an interface. Use the `no` form of this command to stop transmitting LLDP on an interface.

**Syntax**

```
lldp transmit
no lldp transmit
```
Parameters
N/A

Default Configuration
Enabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are sent on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# lldp transmit
```

39.3 lldp receive

Use the lldp receive Interface Configuration mode command to enable receiving LLDP on an interface. Use the no form of this command to stop receiving LLDP on an interface.

Syntax
lldp receive
no lldp receive

Parameters
N/A

Default Configuration
Enabled
Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
LLDP manages LAG ports individually. LLDP data received through LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. i.e. LLDP frames are received on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# lldp receive
```

39.4 lldp timer

Use the lldp timer Global Configuration mode command to specify how often the software sends LLDP updates. Use the no form of this command to restore the default configuration.

Syntax

```
lldp timer seconds
no lldp timer
```

Parameters

```
timer seconds—Specifies, in seconds, how often the software sends LLDP updates (range: 5-32768 seconds).
```

Default Configuration

30 seconds.

Command Mode

Global Configuration mode
Example

The following example sets the interval for sending LLDP updates to 60 seconds.

```
switchxxxxxx(config)# lldp timer 60
```

39.5 lldp hold-multiplier

Use the `lldp hold-multiplier` Global Configuration mode command to specify how long the receiving device holds a LLDP packet before discarding it. Use the `no` form of this command to restore the default configuration.

Syntax

```
lldp hold-multiplier number
no lldp hold-multiplier
```

Parameters

- `hold-multiplier number`—Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value (range: 2-10).

Default Configuration

The default LLDP hold multiplier is 4.

Command Mode

Global Configuration mode

User Guidelines

The actual Time-To-Live (TTL) value of LLDP frames is calculated by the following formula:

\[ TTL = \min(65535, \text{LLDP-Timer} \times \text{LLDP-hold-multiplier}) \]

For example, if the value of the LLDP timer is 30 seconds, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.
Example
The following example sets the LLDP packet hold time interval to 90 seconds.

```
switchxxxxxx(config)# lldp timer 30
switchxxxxxx(config)# lldp hold-multiplier 3
```

### 39.6 lldp reinit

Use the `lldp reinit` Global Configuration mode command to specify the minimum time an LLDP port waits before reinitializing LLDP transmission. Use the `no` form of this command to revert to the default setting.

**Syntax**

```
lldp reinit seconds
no lldp reinit
```

**Parameters**

*reinit seconds*—Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission. (Range: 1–10)

**Default Configuration**

2 seconds

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# lldp reinit 4
```

### 39.7 lldp tx-delay

Use the `lldp tx-delay` Global Configuration mode command to set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the `no` form of this command to restore the default configuration.
Syntax
lldp tx-delay seconds
no lldp tx-delay

Parameters

**tx-delay seconds**—Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB (range: 1-8192 seconds).

Default Configuration

The default LLDP frame transmission delay is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended that the tx-delay be less than 0.25 of the LLDP timer interval.

Example

The following example sets the LLDP transmission delay to 10 seconds.

```
switchxxxxxx(config)# lldp tx-delay 10
```

### 39.8  lldp optional-tlv

Use the lldp optional-tlv Interface Configuration (Ethernet) mode command to specify which optional TLVs are transmitted. Use the no form of this command to restore the default configuration.

For 802.1, see the lldp optional-tlv 802.1 command.

Syntax

lldp optional-tlv tlv[tlv2 ... tlv5 | none]
Parameters

- **tlv**—Specifies the TLVs to be included. Available optional TLVs are:
  port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag,
  802.3-max-frame-size.
- **none**—Clear all optional TLVs from the interface.

If the 802.1 protocol is selected, see the command below.

**Default Configuration**

The system capabilities (sys-cap) optional TLV and the system name (sys-name)
optional TLV are transmitted

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example specifies that the port description TLV is transmitted on
`gi1/1/2`.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# lldp optional-tlv port-desc
```

### 39.9 **lldp optional-tlv 802.1**

Use the `lldp optional-tlv 802.1` Interface Configuration mode command to specify
which optional TLVs to transmit. Use the **no** form of this command to revert to the
default setting.

**Syntax**

- `lldp optional-tlv 802.1 pvid` - The PVID is advertised.
- `no lldp optional-tlv 802.1 pvid` - The PVID is not advertised
- `lldp optional-tlv 802.1 ppvid add ppvid` - The Protocol Port VLAN ID (PPVID) is
  advertised. The PPVID is the PVID that is used depending on the packet’s protocol.
- `lldp optional-tlv 802.1 ppvid remove ppvid` - The PPVID is not advertised.
- `lldp optional-tlv 802.1 vlan add vlan-id` - This `vlan-id` is advertised.
lldp optional-tlv 802.1 vlan remove vlan-id - This vlan-id is not advertised.

lldp optional-tlv 802.1 protocol add {stp / rstp / mstp / pause / 802.1x / lacp / gvrp} - The protocols selected are advertised.

lldp optional-tlv 802.1 protocol remove {stp / rstp / mstp / pause / 802.1x / lacp / gvrp} - The protocols selected are not advertised.

Parameters

- lldp optional-tlv 802.1 pvid—Advertises the PVID of the port.
- lldp optional-tlv 802.1 ppvid add/remove ppvid—Adds/removes PPVID for advertising. (range: 0–4094). PPVID = 0 indicates that the port is not capable of supporting port and protocol VLANs and/or the port is not enabled with any protocol VLANs.
- add/remove vlan-id—Adds/removes VLAN for advertising (range: 0–4094).
- add/remove {stp / rstp / mstp / pause / 802.1x / lacp / gvrp}—Add specifies to advertise the specified protocols; remove specifies not to advertise the specified protocol.

Default Configuration

The PVID optional TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

Example

switchxxxxxx(config)# lldp optional-tlv 802.1 protocol add stp

39.10 lldp management-address

Use the lldp management-address Interface Configuration (Ethernet) mode command to specify the management address advertised by an interface. Use the no form of this command to stop advertising management address information.

Syntax

lldp management-address {ip-address / none / automatic [interface-id]}

no lldp management-address
Parameters

- **ip-address**—Specifies the static management address to advertise.
- **none**—Specifies that no address is advertised.
- **automatic**—Specifies that the software automatically selects a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses.
- **automatic interface-id**—(Available only when the device is in Layer 3 (router mode)). Specifies that the software automatically selects a management address to advertise from the IP addresses that are configured on the interface ID. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN. Note that if the port or port-channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

Default Configuration

No IP address is advertised.

The default advertisement is **automatic**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to **automatic** on gi1/1/2.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# lldp management-address automatic
```
39.11 lldp notifications

Use the `lldp notifications` Interface Configuration (Ethernet) mode command to enable/disable sending LLDP notifications on an interface. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
lldp notifications {enable | disable}
no lldp notifications
```

**Parameters**

- `enable`—Enables sending LLDP notifications.
- `disable`—Disables sending LLDP notifications.

**Default Configuration**

Disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example enables sending LLDP notifications on gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# lldp notifications enable
```

39.12 lldp notifications interval

Use the `lldp notifications interval` Global Configuration mode command to configure the maximum transmission rate of LLDP notifications. Use the `no` form of this command to return to the default.

**Syntax**

```
lldp notifications interval seconds
no lldp notifications interval
```

---

568: 

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# lldp notifications enable
```
Parameters

interval seconds—The device does not send more than a single notification in the indicated period (range: 5–3600).

Default Configuration

5 seconds

Command Mode

Global Configuration mode

Example

switchxxxxxx(config)# lldp notifications interval 10

39.13 lldp lldpdu

The lldp lldpdu Global Configuration mode command defines LLDP packet handling when LLDP is globally disabled. To restore the default configuration, use the no form of this command.

Syntax

lldp lldpdu {filtering | flooding}

no lldp lldpdu

Parameters

- filtering—Specifies that when LLDP is globally disabled, LLDP packets are filtered (deleted).
- flooding—Specifies that when LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).

Default Configuration

LLDP packets are filtered when LLDP is globally disabled.

Command Mode

Global Configuration mode
User Guidelines

If the STP mode is MSTP, the LLDP packet handling mode cannot be set to flooding.

The STP mode cannot be set to MSTP if the LLDP packet handling mode is flooding.

If LLDP is globally disabled, and the LLDP packet handling mode is flooding, LLDP packets are treated as data packets with the following exceptions:

- VLAN ingress rules are not applied to LLDP packets. The LLDP packets are trapped on all ports for which the STP state is Forwarding.
- Default "deny-all" rules are not applied to LLDP packets.
- VLAN egress rules are not applied to LLDP packets. The LLDP packets are flooded to all ports for which the STP state is Forwarding.
- LLDP packets are sent as untagged.

Example

The following example sets the LLDP packet handling mode to Flooding when LLDP is globally disabled.

```
switchxxxxxx(config)# lldp lldpdu flooding
```

39.14 lldp med

Use the lldp med Interface Configuration (Ethernet) mode command to enable or disable LLDP Media Endpoint Discovery (MED) on a port. Use the no form of this command to return to the default state.

Syntax

```
lldp med {enable [tlv ... tlv4] | disable}
```

Parameters

- `enable` - Enable LLDP MED
- `tlv`—Specifies the TLV that should be included. Available TLVs are: network-policy, location, and poe-pse, inventory. The capabilities TLV is always included if LLDP-MED is enabled.
- **disable** - disable LLDP MED on the port

Default Configuration

Enabled with network-policy TLV

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables LLDP MED with the **location** TLV on gi1/1/3.

```
switchxxxxxx(config)# interface gi1/1/3
switchxxxxxx(config-if)# lldp med enable location
```

### 39.15 lldp med notifications topology-change

Use the **lldp med notifications topology-change** Interface Configuration (Ethernet) mode command to enable sending LLDP MED topology change notifications on a port. Use the no form of this command to restore the default configuration.

**Syntax**

```
lldp med notifications topology-change {enable | disable}
no lldp med notifications topology-change
```

**Parameters**

- **enable**—Enables sending LLDP MED topology change notifications.
- **disable**—Disables sending LLDP MED topology change notifications.

Default Configuration

Disable is the default.

Command Mode

Interface Configuration (Ethernet) mode
Example

The following example enables sending LLDP MED topology change notifications on gi1/1/2.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# lldp med notifications topology-change enable
```

### 39.16 lldp med fast-start repeat-count

When a port comes up, LLDP can send packets more quickly than usual using its fast-start mechanism.

Use the `lldp med fast-start repeat-count` Global Configuration mode command to configure the number of packets that is sent during the activation of the fast start mechanism. Use the `no` form of this command return to default.

**Syntax**

```
lldp med fast-start repeat-count number
no lldp med fast-start repeat-count
```

**Parameters**

- `repeat-count number`—Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism. The range is 1-10.

**Default Configuration**

3

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# lldp med fast-start repeat-count 4
```
39.17  lldp med network-policy (global)

Use the lldp med network-policy Global Configuration mode command to define a LLDP MED network policy. For voice applications, it is simpler to use lldp med network-policy voice auto.

The lldp med network-policy command creates the network policy, which is attached to a port by lldp med network-policy (interface).

The network policy defines how LLDP packets are constructed.

Use the no form of this command to remove LLDP MED network policy.

Syntax

lldp med network-policy number application [vlan vlan-id] [vlan-type {tagged | untagged}] [up priority] [dscp value]

no lldp med network-policy number

Parameters

- **number**—Network policy sequential number. The range is 1-32.
- **application**—The name or the number of the primary function of the application defined for this network policy. Available application names are:
  - voice
  - voice-signaling
  - guest-voice
  - guest-voice-signaling
  - softphone-voice
  - video-conferencing
  - streaming-video
  - video-signaling.
- **vlan vlan-id**—VLAN identifier for the application.
- **vlan-type**—Specifies if the application is using a tagged or an untagged VLAN.
- **up priority**—User Priority (Layer 2 priority) to be used for the specified application.
- **dscp value**—DSCP value to be used for the specified application.

**Default Configuration**

No network policy is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `lldp med network-policy` Interface Configuration command to attach a network policy to a port.

Up to 32 network policies can be defined.

**Example**

This example creates a network policy for the voice-signaling application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1
          vlan-type untagged up 1 dscp 2
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

### 39.18 lldp med network-policy (interface)

Use the `lldp med network-policy` Interface Configuration (Ethernet) mode command to attach or remove an LLDP MED network policy on a port. Network policies are created in `lldp med network-policy (global)`.

Use the `no` form of this command to remove all the LLDP MED network policies from the port.

**Syntax**

```
lldp med network-policy {add | remove} number
no lldp med network-policy number
```
Link Layer Discovery Protocol (LLDP) Commands

Parameters

- **number**—Specifies the network policy sequential number. The range is 1-32
- **add/remove number**—Attaches/removes the specified network policy to the interface.

Default Configuration

No network policy is attached to the interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

For each port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

Example

This example creates a network policy for the voice-signaling application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1
vlan-type untagged up 1 dscp 2
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

### 39.19  **lldp med network-policy voice auto**

A network policy for voice LLDP packets can be created by using the **lldp med network-policy (global)**. The **lldp med network-policy voice auto** Global Configuration mode is simpler in that it uses the configuration of the Voice application to create the network policy instead of the user having to manually configure it.

This command generates an LLDP MED network policy for voice, if the voice VLAN operation mode is **auto voice VLAN**. The voice VLAN, 802.1p priority, and the DSCP of the voice VLAN are used in the policy. Use the **no** form of this command.
to disable this mode. The network policy is attached automatically to the voice VLAN.

Syntax

lldp med network-policy voice auto
no lldp med network-policy voice auto

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

In Auto mode, the Voice VLAN feature determines on which interfaces to advertise the network policy TLV with application type voice, and controls the parameters of that TLV.

To enable the auto generation of a network policy based on the auto voice VLAN, there must be no manual pre-configured network policies for the voice application

In Auto mode, you cannot manually define a network policy for the voice application using the lldp med network-policy (global) command.

Example

```
switchxxxxxx(config)# lldp med network-policy voice auto
```

### 39.20 clear lldp table

Use the clear lldp table command in Privileged EXEC mode to clear the neighbors table for all ports or for a specific port.

Syntax

```
clear lldp table [interface-id]
```
Parameters

interface-id—Specifies a port ID.

Default Configuration

If no interface is specified, the default is to clear the LLDP table for all ports.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear lldp table gi1/1/1
```

### 39.21 lldp med location

Use the `lldp med location` Interface Configuration (Ethernet) mode command to configure the location information for the LLDP Media Endpoint Discovery (MED) for a port. Use the `no` form of this command to delete location information for a port.

**Syntax**

```
lldp med location {{coordinate data} | {civic-address data} | {ecs-elin data}}
```

```
no lldp med location {coordinate | civic-address | ecs-elin}
```

**Parameters**

- `coordinate data`—Specifies the location data as coordinates in hexadecimal format.
- `civic-address data`—Specifies the location data as a civic address in hexadecimal format.
- `ecs-elin data`—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN) in hexadecimal format.
- `data`—Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)
Default Configuration

The location is not configured.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example configures the LLDP MED location information on gi1/1/2 as a civic address.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# lldp med location civic-address 616263646566
```

39.22 lldp chassis-id

Use the lldp chassis-id Global Configuration mode command to configure the source of the chassis ID of the port. Use the no form of this command to restore the chassis ID source to default.

Syntax

```
lldp chassis-id {mac-address | host-name}
no lldp chassis-id
```

Parameters

- `mac-address`—Specifies the chassis ID to use the device MAC address.
- `host-name`—Specifies the chassis ID to use the device configured host name.

Default Configuration

MAC address.

Command Mode

Global Configuration mode
User Guidelines

The host name should be configured to be a unique value.

If the chassis ID configured to be used in LLDP packets is empty, LLDP uses the default chassis ID (specified above).

Example

The following example configures the chassis ID to be the MAC address.

```
switchxxxxx(config)# lldp chassis-id mac-address
```

39.23 show lldp configuration

Use the `show lldp configuration` Privileged EXEC mode command to display the LLDP configuration for all ports or for a specific port.

Syntax

```
show lldp configuration [interface-id | detailed]
```

Parameters

- `interface-id`—Specifies the port ID.
- `detailed`—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - Display LLDP configuration for all ports.

```
Switch# show lldp configuration
State: Enabled
Timer: 30 Seconds
```
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Optional TLVs</th>
<th>Address</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1</td>
<td>RX,TX</td>
<td>PD, SN, SD, SC</td>
<td>172.16.1.1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/2</td>
<td>TX</td>
<td>PD, SN</td>
<td>172.16.1.1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/3</td>
<td>RX,TX</td>
<td>PD, SN, SD, SC</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/5</td>
<td>RX,TX</td>
<td>D, SN, SD, SC</td>
<td>automatic</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/6</td>
<td>RX,TX</td>
<td>PD, SN, SD, SC</td>
<td>auto vlan 1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/7</td>
<td>RX,TX</td>
<td>PD, SN, SD, SC</td>
<td>auto g1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi1/8</td>
<td>RX,TX</td>
<td>PD, SN, SD, SC</td>
<td>auto ch1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Example 2 - Display LLDP configuration for port 1.

```
Switch# show lldp configuration gi1/1/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Chassis ID: mac-address

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Optional TLVs</th>
<th>Address</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>72.16.1.1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```

802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
<td>The time interval between LLDP updates.</td>
</tr>
<tr>
<td>Hold multiplier</td>
<td>The amount of time (as a multiple of the timer interval) that the receiving device holds a LLDP packet before discarding it.</td>
</tr>
<tr>
<td>Reinit timer</td>
<td>The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.</td>
</tr>
<tr>
<td>Tx delay</td>
<td>The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>State</td>
<td>The port's LLDP state.</td>
</tr>
<tr>
<td>Optional TLVs</td>
<td>Optional TLVs that are advertised. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>PD - Port description</td>
</tr>
<tr>
<td></td>
<td>SN - System name</td>
</tr>
<tr>
<td></td>
<td>SD - System description</td>
</tr>
<tr>
<td></td>
<td>SC - System capabilities</td>
</tr>
<tr>
<td>Address</td>
<td>The management address that is advertised.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Indicates whether LLDP notifications are enabled or disabled.</td>
</tr>
<tr>
<td>PVID</td>
<td>Port VLAN ID advertised.</td>
</tr>
<tr>
<td>PPVID</td>
<td>Protocol Port VLAN ID advertised.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Protocols advertised.</td>
</tr>
</tbody>
</table>

39.24 show lldp med configuration

Use the `show lldp med configuration` Privileged EXEC mode command to display the LLDP Media Endpoint Discovery (MED) configuration for all ports or for a specific port.
Syntax

show lldp med configuration [interface-id | detailed]

Parameters

- interface-id—Specifies the port ID.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays the LLDP MED configuration for all interfaces.

```
switchxxxxxx# show lldp med configuration
Fast Start Repeat Count: 4.
lldp med network-policy voice: manual
Network policy 1

Application type: voiceSignaling
VLAN ID: 1  untagged
Layer 2 priority: 0
DSCP: 0

Port       Capabilities  Network Policy Location  Notifications  Inventory
---------- -------------- -------------- ---------- -------------   --------
gi1/1/1    Yes             Yes            Yes         Enabled        Yes
```
Example 2 - The following example displays the LLDP MED configuration for gi1/1/1.

switchxxxxxx# show lldp med configuration gi1/1/1

Port  Capabilities  Network Policy  Location  Notifications  Inventory
-------  --------------  ----------------  ---------  ----------  --------
gi1/1/1  Yes  Yes  Yes  Enabled  Yes

Network policies:
Location:

39.25  show lldp local tlvs-overloading

When an LLDP packet contains too much information for one packet, this is called overloading. Use the show lldp local tlvs-overloading EXEC mode command to display the status of TLVs overloading of the LLDP on all ports or on a specific port.

Syntax

show lldp local tlvs-overloading [interface-id]

Parameters

interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

EXEC mode

User Guidelines

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.
39.26  show lldp local

Use the show lldp local Privileged EXEC mode command to display the LLDP information that is advertised from a specific port.

Syntax

show lldp local interface-id

Parameters

Interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

Example

The following examples display LLDP information that is advertised from gi1/1/1 and 2.

Switch# show lldp local gi1/1/1
Device ID: 0060.704C.73FF
Port ID: gi1/1/1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MACPHY ConfigurationStatus
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123
Switch# show lldp local gi1/1/2
LLDP is disabled.

39.27 show lldp neighbors

Use the show lldp neighbors Privileged EXEC mode command to display information about neighboring devices discovered using LLDP. The information can be displayed for all ports or for a specific port.

Syntax

show lldp neighbors [interface-id]

Parameters

interface-id—Specifies a port ID.
Default Configuration
If no port ID is entered, the command displays information for all ports.

Command Mode
Privileged EXEC mode

User Guidelines
A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Examples
Example 1 - The following example displays information about neighboring devices discovered using LLDP on all ports on which LLDP is enabled and who are up.
Location information, if it exists, is also displayed.

Switch# show lldp neighbors

System capability legend:
B - Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other

<table>
<thead>
<tr>
<th>Port</th>
<th>Device ID</th>
<th>Port ID</th>
<th>System Name</th>
<th>Capabilities</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1</td>
<td>00:00:00:11:11:11</td>
<td>gi1/1/1</td>
<td>ts-7800-2</td>
<td>B</td>
<td>90</td>
</tr>
<tr>
<td>gi1/1</td>
<td>00:00:00:11:11:11</td>
<td>gi1/1/1</td>
<td>ts-7800-2</td>
<td>B</td>
<td>90</td>
</tr>
<tr>
<td>gi1/2</td>
<td>00:00:26:08:13:24</td>
<td>gi1/1/3</td>
<td>ts-7900-1</td>
<td>B, R</td>
<td>90</td>
</tr>
<tr>
<td>gi1/3</td>
<td>00:00:26:08:13:24</td>
<td>gi1/1/2</td>
<td>ts-7900-2</td>
<td>W</td>
<td>90</td>
</tr>
</tbody>
</table>

Example 2 - The following example displays information about neighboring devices discovered using LLDP on port 1.

Switch# show lldp neighbors gi1/1/1
Device ID: 00:00:00:11:11:11
Port ID: gi1/1/1
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds
802.3 MACPHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD
802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2(VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.
LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
LLDP-MED Location

The following table describes significant LLDP fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The neighbor device’s configured ID (name) or MAC address.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port ID</td>
<td>The neighbor device’s port ID.</td>
</tr>
<tr>
<td>System name</td>
<td>The neighbor device’s administratively assigned name.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The capabilities discovered on the neighbor device. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>B - Bridge</td>
</tr>
<tr>
<td></td>
<td>R - Router</td>
</tr>
<tr>
<td></td>
<td>W - WLAN Access Point</td>
</tr>
<tr>
<td></td>
<td>T - Telephone</td>
</tr>
<tr>
<td></td>
<td>D - DOCSIS cable device</td>
</tr>
<tr>
<td></td>
<td>H - Host</td>
</tr>
<tr>
<td></td>
<td>r - Repeater</td>
</tr>
<tr>
<td></td>
<td>O - Other</td>
</tr>
<tr>
<td>System description</td>
<td>The neighbor device’s system description.</td>
</tr>
<tr>
<td>Port description</td>
<td>The neighbor device’s port description.</td>
</tr>
<tr>
<td>Management address</td>
<td>The neighbor device’s management address.</td>
</tr>
<tr>
<td>Auto-negotiation support</td>
<td>The auto-negotiation support status on the port. (supported or not supported)</td>
</tr>
<tr>
<td>Auto-negotiation status</td>
<td>The active status of auto-negotiation on the port. (enabled or disabled)</td>
</tr>
<tr>
<td>Auto-negotiation Advertised Capabilities</td>
<td>The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.</td>
</tr>
<tr>
<td>Operational MAU type</td>
<td>The port MAU type.</td>
</tr>
<tr>
<td>LLDP MED</td>
<td></td>
</tr>
<tr>
<td>Capabilities</td>
<td>The sender’s LLDP-MED capabilities.</td>
</tr>
<tr>
<td>Device type</td>
<td>The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.</td>
</tr>
<tr>
<td>LLDP MED - Network Policy</td>
<td></td>
</tr>
<tr>
<td>Application type</td>
<td>The primary function of the application defined for this network policy.</td>
</tr>
</tbody>
</table>
### Flags
Flags. The possible values are:
- **Unknown policy**: Policy is required by the device, but is currently unknown.
- **Tagged VLAN**: The specified application type is using a tagged VLAN.
- **Untagged VLAN**: The specified application type is using an untagged VLAN.

### VLAN ID
The VLAN identifier for the application.

### Layer 2 priority
The Layer 2 priority used for the specified application.

### DSCP
The DSCP value used for the specified application.

### LLDP MED - Power Over Ethernet

#### Power type
The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).

#### Power Source
The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.

#### Power priority
The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.

#### Power value
The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

### LLDP MED - Location

#### Coordinates, Civic address, ECS ELIN
The location information raw data.
39.28  show lldp statistics

Use the show lldp statistics EXEC mode command to display LLDP statistics on all ports or a specific port.

Syntax

show lldp statistics [interface-id | detailed]

Parameters

- interface-id—Specifies the port ID.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

switchxxxxxx# show lldp statistics

Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1

+----------+---------+---------+---------+---------+---------+---------+---------+
<table>
<thead>
<tr>
<th>Port</th>
<th>TX Frames</th>
<th>RX Frame</th>
<th>RX TLVs</th>
<th>RX Ageouts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/1</td>
<td>730</td>
<td>850</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/1/3</td>
<td>730</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
+----------+---------+---------+---------+---------+
The following table describes significant LLDP fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The neighbor device’s configured ID (name) or MAC address.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The neighbor device’s port ID.</td>
</tr>
<tr>
<td>System name</td>
<td>The neighbor device’s administratively assigned name.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The capabilities discovered on the neighbor device. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>B - Bridge</td>
</tr>
<tr>
<td></td>
<td>R - Router</td>
</tr>
<tr>
<td></td>
<td>W - WLAN Access Point</td>
</tr>
<tr>
<td></td>
<td>T - Telephone</td>
</tr>
<tr>
<td></td>
<td>D - DOCSIS cable device</td>
</tr>
<tr>
<td></td>
<td>H - Host</td>
</tr>
<tr>
<td></td>
<td>r - Repeater</td>
</tr>
<tr>
<td></td>
<td>O - Other</td>
</tr>
<tr>
<td>System description</td>
<td>The neighbor device’s system description.</td>
</tr>
<tr>
<td>Port description</td>
<td>The neighbor device’s port description.</td>
</tr>
<tr>
<td>Management address</td>
<td>The neighbor device’s management address.</td>
</tr>
<tr>
<td>Auto-negotiation support</td>
<td>The auto-negotiation support status on the port. (Supported or Not Supported)</td>
</tr>
<tr>
<td>Auto-negotiation status</td>
<td>The active status of auto-negotiation on the port. (Enabled or Disabled)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Auto-negotiation Advertised Capabilities</strong></td>
<td>The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.</td>
</tr>
<tr>
<td><strong>Operational MAU type</strong></td>
<td>The port MAU type.</td>
</tr>
<tr>
<td><strong>LLDP MED</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td>The sender's LLDP-MED capabilities.</td>
</tr>
<tr>
<td><strong>Device type</strong></td>
<td>The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.</td>
</tr>
<tr>
<td><strong>LLDP MED - Network Policy</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Application type</strong></td>
<td>The primary function of the application defined for this network policy.</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Flags. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>Unknown policy: Policy is required by the device, but is currently unknown.</td>
</tr>
<tr>
<td></td>
<td>Tagged VLAN: The specified application type is using a Tagged VLAN.</td>
</tr>
<tr>
<td></td>
<td>Untagged VLAN: The specified application type is using an Untagged VLAN.</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td>The VLAN identifier for the application.</td>
</tr>
<tr>
<td><strong>Layer 2 priority</strong></td>
<td>The Layer 2 priority used for the specified application.</td>
</tr>
<tr>
<td><strong>DSCP</strong></td>
<td>The DSCP value used for the specified application.</td>
</tr>
<tr>
<td><strong>LLDP MED - Power Over Ethernet</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Power type</strong></td>
<td>The device power type. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>Power Sourcing Entity (PSE) or Power Device (PD).</td>
</tr>
<tr>
<td><strong>Power Source</strong></td>
<td>The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.</td>
</tr>
<tr>
<td><strong>Power priority</strong></td>
<td>The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power value</td>
<td>The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.</td>
</tr>
<tr>
<td><strong>LLDP MED - Location</strong></td>
<td></td>
</tr>
<tr>
<td>Coordinates, Civic address, ECS ELIN.</td>
<td>The location information raw data.</td>
</tr>
</tbody>
</table>
IGMP Snooping Commands

40.1 ip igmp snooping (Global)

Use the ip igmp snooping Global Configuration mode command to enable Internet
Group Management Protocol (IGMP) snooping. Use the no form of this command
to disable IGMP snooping.

Syntax

ip igmp snooping
no ip igmp snooping

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

switchxxxxxx(config)# ip igmp snooping

40.2 ip igmp snooping vlan

Use the ip igmp snooping vlan Global Configuration mode command to enable
IGMP snooping on a specific VLAN. Use the no form of this command to disable
IGMP snooping on a VLAN interface.

Syntax

ip igmp snooping vlan vlan-id
no ip igmp snooping vlan vlan-id
Parameters

vlan vlan-id—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2, and IGMPv3 Snooping are supported.

To activate IGMP snooping, the bridge multicast filtering should be enabled.

The user guidelines of the bridge multicast mode Interface VLAN Configuration command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

40.3  ip igmp snooping vlan mrouter

Use the ip igmp snooping vlan mrouter Global Configuration mode command to enable automatic learning of Multicast router ports on a VLAN. Use the no form of this command to remove the configuration.

Syntax

ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp

no ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp

Parameters

vlan vlan-id—Specifies the VLAN.

Default Configuration

Learning pim-dvmrp is enabled.
**Command Mode**
Global Configuration mode

**User Guidelines**
Multicast router ports are learned according to:
- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MRDISC received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

### 40.4 `ip igmp snooping vlan mrouter interface`

Use the `ip igmp snooping mrouter interface` Global Configuration mode command to define a port that is connected to a Multicast router port. Use the `no` form of this command to remove the configuration.

**Syntax**

```
ip igmp snooping vlan vlan-id mrouter interface interface-list
no ip igmp snooping vlan vlan-id mrouter interface interface-list
```

**Parameters**

- `vlan vlan-id`—Specifies the VLAN.
- `interface interface-list`—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

**Default Configuration**

No ports defined
**Command Mode**

Global Configuration mode

**User Guidelines**

A port that is defined as a Multicast router port receives all IGMP packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interface gi1/1/1
```

### 40.5 ip igmp snooping vlan forbidden mrouter

Use the `ip igmp snooping vlan forbidden mrouter` Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the `no` form of this command to remove the configuration.

**Syntax**

```
ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list
no ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list
```

**Parameters**

- `vlan vlan-id`—Specifies the VLAN.
- `interface interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**Default Configuration**

No ports defined.

**Command Mode**

Global Configuration mode
User Guidelines

A port that is a forbidden mrouter port cannot be a Multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden mrouter interface gi1/1/1
```

**40.6 ip igmp snooping vlan static**

Use the `ip igmp snooping vlan static` Global Configuration mode command to register an IP-layer Multicast address to the bridge table, and to add static ports to the group defined by this address. Use the `no` form of this command to remove ports specified as members of a static Multicast group.

Syntax

```
ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
no ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

Parameter

- `vlan vlan-id`—Specifies the VLAN.
- `static ip-address`—Specifies the IP Multicast address.
- `interface interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static Multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.
You can register an entry without specifying an interface. Using the no command without a port-list removes the entry.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface gi1/1/1
```

### 40.7 ip igmp snooping vlan multicast-tv

Use the `ip igmp snooping vlan multicast-tv` Global Configuration mode command to define the Multicast IP addresses that are associated with a Multicast TV VLAN. Use the no form of this command to remove all associations.

**Syntax**

```
ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]
no ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]
```

**Parameters**

- `vlan-id`—Specifies the VLAN
- `count number`—Configures multiple contiguous Multicast IP addresses. If not specified, the default is 1. (Range: 1–256)

**Default Configuration**

No Multicast IP address is associated.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command to define the Multicast transmissions on a Multicast-TV VLAN. The configuration is only relevant for an Access port that is a member in the configured VLAN as a Multicast-TV VLAN.

If an IGMP message is received on such an Access port, it is associated with the Multicast-TV VLAN only if it is for one of the Multicast IP addresses that are associated with the Multicast-TV VLAN.
Up to 256 VLANs can be configured.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 multicast-tv 239.2.2.2 count 3
```

### 40.8 ip igmp snooping map cpe vlan

The `ip igmp snooping map cpe vlan` Global Configuration mode command maps CPE VLANs to Multicast-TV VLANs. Use the `no` form of this command to remove the mapping.

**Syntax**

```
ip igmp snooping map cpe vlan vlan-id multicast-tv vlan vlan-id
no ip igmp snooping map cpe vlan vlan-id
```

**Parameters**

- `cpe vlan vlan-id`—Specifies the CPE VLAN ID.
- `multicast-tv vlan vlan-id`—Specifies the Multicast-TV VLAN ID.

**Default Configuration**

No mapping exists.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command to associate the CPE VLAN with a Multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is mapping from that CPE VLAN to a Multicast-TV VLAN, the IGMP message is associated with the Multicast-TV VLAN.

**Example**

The following example maps CPE VLAN 2 to Multicast-TV VLAN 31.

```
switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan 31
```
40.9  ip igmp snooping querier address

Use the `ip igmp snooping querier address` Global Configuration mode command to define globally the source IP address that the IGMP snooping querier uses. Use the `no` form of this command to return to default.

**Syntax**

```
ip igmp snooping querier address ip-address
no ip igmp snooping querier address
```

**Parameters**

- `querier address ip-address`—Source IP address.

**Default Configuration**

No IP address

**Command Mode**

Global Configuration mode

**User Guidelines**

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If it is not configured for the VLAN and an IP address is configured globally, it is used as the source address of the IGMP snooping querier. If an IP address is not configured for the VLAN and is not configured globally, the minimum IP address defined on the VLAN is used.

If an IP address is not configured for the VLAN and is not configured globally and no IP address is defined on the VLAN, the querier is disabled.

**Example**

The following example define IP address 10.5.234.205 as the Querier Snooping IP address on a VLAN if it is not configured for the VLAN.

```
switchxxxxxx(config)# ip igmp snooping querier address 10.5.234.205
```
40.10  ip igmp snooping vlan querier

Use the ip igmp snooping vlan querier Global Configuration mode command to enable the IGMP Snooping querier on a specific VLAN. Use the no form of this command to disable the IGMP Snooping querier on a VLAN interface.

Syntax

ip igmp snooping vlan vlan-id querier

no ip igmp snooping vlan vlan-id querier

Parameters

vlan vlan-id—Specifies the VLAN

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The IGMP Snooping querier can be enabled on a VLAN only if IGMP Snooping is enabled for that VLAN.

When the IGMP Snooping querier is enabled, it starts after 60 sec with no IGMP General Query messages being detected from a Multicast router.

Example

The following example enables the IGMP Snooping querier on VLAN 1:

```bash
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

40.11  ip igmp snooping vlan querier address

Use the ip igmp snooping vlan querier address Global Configuration mode command to define the source IP address that the IGMP snooping querier uses. Use the no form of this command to return to default.
**Syntax**

```
ip igmp snooping vlan vlan-id querier address ip-address
no ip igmp snooping vlan vlan-id querier address
```

**Parameters**

- `vlan vlan-id`—Specifies the VLAN.
- `querier address ip-address`—Source IP address.

**Default Configuration**

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

**Command Mode**

Global Configuration mode

**User Guidelines**

If an IP address is not configured by this command, and no IP address is configured for the querier’s VLAN, the querier is disabled.

**Example**

```
switchxxxxx(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

### 40.12 ip igmp snooping vlan querier version

Use the `ip igmp snooping vlan querier version` Global Configuration mode command to configure the IGMP version of an IGMP Snooping querier on a specific VLAN. Use the `no` form of this command to return to the default version.

**Syntax**

```
ip igmp snooping vlan vlan-id querier version {2 | 3}
no ip igmp snooping vlan vlan-id querier version
```

**Parameters**

- `vlan vlan-id`— Specifies the VLAN.
- **querier version 2**—Specifies that the IGMP version would be IGMPv2.
- **querier version 3**—Specifies that the IGMP version would be IGMPv3.

**Default Configuration**

IGMPv2.

**Command Mode**

Global Configuration mode

**Example**

The following example sets the version of the IGMP Snooping Querier VLAN 1 to 3:

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

### 40.13 ip igmp robustness

Use the `ip igmp robustness` Interface Configuration (VLAN) mode command to set the IGMP robustness variable on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```
ip igmp robustness count
no ip igmp robustness
```

**Parameters**

- `count`—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

**Default Configuration**

2

**Command Mode**

Interface Configuration (VLAN) mode
**User Guidelines**

You can execute the command before the VLAN is created, but you must enter the command in Interface VLAN mode.

**Example**

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp robustness 3
```

### 40.14 ip igmp query-interval

Use the `ip igmp query-interval` Interface Configuration (VLAN) mode command to configure the Query interval on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```
ip igmp query-interval seconds
no ip igmp query-interval
```

**Parameters**

- `seconds`—Frequency, in seconds, at which IGMP query messages are sent on the interface. (Range: 30–18000)

**Default Configuration**

125

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp query-interval 200
```
40.15  ip igmp query-max-response-time

Use the `ip igmp query-max-response-time` Interface Configuration (VLAN) mode command to configure the Query Maximum Response time on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

`ip igmp query-max-response-time seconds`

`no ip igmp query-max-response-time`

**Parameters**

`seconds`—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

**Default Configuration**

10

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp query-max-response-time 20
```
Parameter

**count**—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

**Default Configuration**

A value of Robustness variable

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 7
```

### 40.17  **ip igmp last-member-query-interval**

Use the `ip igmp last-member-query-interval` **Interface Configuration (VLAN) mode** command to configure the Last Member Query interval on a VLAN. Use the **no** format of the command to return to default.

**Syntax**

```
ip igmp last-member-query-interval milliseconds
no ip igmp last-member-query-interval
```

**Parameters**

*milliseconds*—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500)

**Default Configuration**

1000
**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-interval 2000
```

### 40.18 ip igmp snooping vlan immediate-leave

Use the `ip igmp snooping vlan immediate-leave` Global Configuration mode command to enable the IGMP Snooping Immediate-Leave processing on a VLAN. Use the `no` format of the command to disable IGMP Snooping Immediate-Leave processing.

**Syntax**

```
ip igmp snooping vlan `vlan-id` immediate-leave
no ip igmp snooping vlan `vlan-id` immediate-leave
```

**Parameters**

`vlan vlan-id`—Specifies the VLAN ID value. (Range: 1–4094)

**Default Configuration**

Disabled

**Command Mode**

Global Configuration mode

**User Guidelines**

You can execute the command before the VLAN is created.
**Example**

The following example enables IGMP snooping immediate-leave feature on VLAN 1.

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

**40.19 show ip igmp snooping mrouter**

The `show ip igmp snooping mrouter` EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

**Syntax**

```
show ip igmp snooping mrouter [interface vlan-id]
```

**Parameters**

- `interface vlan-id`—Specifies the VLAN ID.

**Command Mode**

EXEC mode

**Example**

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000.

```
switchxxxxxx# show ip igmp snooping mrouter interface 1000

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Dynamic</th>
<th>Static</th>
<th>Forbidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>-------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>1000</td>
<td>gi1/1/1</td>
<td>gi1/1/2</td>
<td>gi1/1/3-23</td>
</tr>
</tbody>
</table>
```

**40.20 show ip igmp snooping interface**

The `show ip igmp snooping interface` EXEC mode command displays the IGMP snooping configuration for a specific VLAN.
Syntax

show ip igmp snooping interface vlan-id

Parameters

interface vlan-id—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the IGMP snooping configuration for VLAN 1000

switchxxxxxx# show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping Querier is globally enabled
IGMP snooping querier global address: 194.10.12.56
IGMP Snooping Querier election is enabled
IGMP Snooping Querier address on the VLAN: 194.12.10.166
IGMP Snooping Querier is enabled on the VLAN
IGMP Snooping Querier version: 1
IGMP Snooping admin: Enabled
IGMP Snooping oper: Enabled
Routers IGMP version: 3
Groups that are in IGMP version 2 compatibility mode:
231.2.2.3, 231.2.2.3
Groups that are in IGMP version 1 compatibility mode:
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3
IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
IGMP snooping last immediate leave: enable
Automatic learning of Multicast router ports is enabled

40.21  show ip igmp snooping groups

The show ip igmp snooping groups EXEC mode command displays the Multicast groups learned by the IGMP snooping.

Syntax

show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address] [source ip-address]

Parameters

vlan vlan-id—Specifies the VLAN ID.
address ip-multicast-address—Specifies the IP multicast address.
source ip-address—Specifies the IP source address.

Command Mode

EXEC mode

User Guidelines

To see all Multicast groups learned by IGMP snooping, use the show ip igmp snooping groups command without parameters.

Use the show ip igmp snooping groups command with parameters to see a needed subset of all Multicast groups learned by IGMP snooping

To see the full Multicast address table (including static addresses), use the show bridge multicast address-table command.
Example

The following example shows sample output for IGMP version 2.

```
switchxxxxx# show ip igmp snooping multicast-tv

VLAN  Group Address  Source Address  Include Ports  Exclude Ports  Comp-Mode
    ----  --------------  --------------  ----------  --------------  --------
1   239.255.255.250  *             gi1           v2
```

40.22  show ip igmp snooping multicast-tv

The `show ip igmp snooping multicast-tv` EXEC mode command displays the IP addresses associated with Multicast TV VLANs.

Syntax

```
show ip igmp snooping multicast-tv [vlan vlan-id]
```

Parameters

`vlan vlan-id`—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the IP addresses associated with all Multicast TV VLANs.

```
switchxxxxx# show ip igmp snooping multicast-tv

VLAN  IP Address
    ----  --------------
1000  239.255.0.0
1000  239.255.0.1
1000  239.255.0.2
1000  239.255.0.3
1000  239.255.0.4
```
The show ip igmp snooping cpe vlans EXEC mode command displays the CPE VLAN to Multicast TV VLAN mappings.

Syntax

show ip igmp snooping cpe vlans [vlan vlan-id]

Parameters

vlan vlan-id — Specifies the CPE VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the CPE VLAN to Multicast TV VLAN mappings.

switchxxxxxx# show ip igmp snooping cpe vlans

CPE VLAN  Multicast-TV VLAN
         ---------  ---------------
  2     1118
  3     1119
41 IPv6 MLD Snooping Commands

41.1 ipv6 mld snooping (Global)

The `ipv6 mld snooping` Global Configuration mode command enables IPv6 Multicast Listener Discovery (MLD) snooping. To disable IPv6 MLD snooping, use the `no` form of this command.

**Syntax**

`ipv6 mld snooping`

`no ipv6 mld snooping`

**Parameters**

N/A

**Default Configuration**
IPv6 MLD snooping is disabled.

**Command Mode**
Global Configuration mode

**Example**

The following example enables IPv6 MLD snooping.

```
switchxxxxxx(config)# ipv6 mld snooping
```

41.2 ipv6 mld snooping vlan

Use the `ipv6 mld snooping vlan` Global Configuration mode command to enable MLD snooping on a specific VLAN. Use the `no` form of this command to disable MLD snooping on a VLAN interface.

**Syntax**

`ipv6 mld snooping vlan vlan-id`
no ipv6 mld snooping vlan vlan-id

Parameters

vlan-id—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

MLD snooping can only be enabled on static VLANs.
MLDv1 and MLDv2 are supported.

To activate MLD snooping, the Bridge Multicast Filtering command must be enabled.

The user guidelines of the bridge multicast ipv6 mode Interface VLAN Configuration command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

Example

switchxxxxxx(config)# ipv6 mld snooping vlan 2

41.3 ipv6 mld robustness

Use the ipv6 mld robustness interface Configuration mode command to change a value of MLD robustness. Use the no format of the command to return to default.

Syntax

ipv6 mld robustness count
no ipv6 mld robustness

Parameters

count - The number of expected packet losses on a link. (Range: 1–7)
Default Configuration

2

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

```
switchxxxxx(config)# interface vlan 1
switchxxxxx(config-if)# ipv6 mld robustness 3
```

41.4 ipv6 mld snooping vlan mrouter

Use the `ipv6 mld snooping vlan mrouter` Global Configuration mode command to enable automatic learning of Multicast router ports. Use the `no` form of this command to remove the configuration.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
no ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `pim-dvmrp`—Learn Multicast router port by PIM, DVMRP and MLD messages.

Default Configuration

Learning `pim-dvmrp` is enabled.

Command Mode
Global Configuration mode
User Guidelines

Multicast router ports can be configured statically with the `bridge multicast forward-all` command.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

### 41.5 `ipv6 mld snooping vlan mrouter`

Use the `ipv6 mld snooping vlan mrouter` Interface Configuration mode command to define a port that is connected to a Multicast router port. Use the `no` form of this command to remove the configuration.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter interface interface-list
no ipv6 mld snooping vlan vlan-id mrouter interface interface-list
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: port or port-channel.

Default Configuration

No ports defined

Command Mode

Interface Configuration mode

User Guidelines

This command may be used in conjunction with the `bridge multicast forward-all` command, which is used in older versions to statically configure a port as a Multicast router.

A port that is defined as a Multicast router port receives all MLD packets (reports and queries) as well as all Multicast data.
You can execute the command before the VLAN is created and for a range of ports as shown in the example.

**Example**

```
switchxxxxxx(config)interface gi1/1/1/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface gi1/1/1/1
```

### 41.6 **ipv6 mld snooping vlan forbidden mrouter**

Use the `ipv6 mld snooping vlan forbidden mrouter` Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the `no` form of this command to remove the configuration.

**Syntax**

```
ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list
no ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list
```

**Parameters**

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**Default Configuration**

No forbidden ports by default

**Command Mode**

Global Configuration mode

**User Guidelines**

A port that is forbidden to be defined as a Multicast router port (mrouter port) cannot be learned dynamically or assigned statically.

The `bridge multicast forbidden forward-all` command was used in older versions to forbid dynamic learning of Multicast router ports.
You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface gi1/1/1
```

4.7.1 `ipv6 mld snooping vlan static`

Use the `ipv6 mld snooping vlan static` Global Configuration mode command to register a IPv6-layer Multicast address to the bridge table, and to add statically ports to the group. Use the `no` form of this command to remove ports specified as members of a static Multicast group.

Syntax

```
ipv6 mld snooping vlan vlan-id static ipv6-address interface [interface-list]
no ipv6 mld snooping vlan vlan-id static ipv6-address interface [interface-list]
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `ipv6-address`—Specifies the IP multicast address
- `interface-list`—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global configuration mode

User Guidelines

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the `no` command without a port-list removes the entry.


Example

switchxxxxxx(config)# ipv6 mld snooping vlan 1 static 239.2.2.2 gi1/1/1

41.8 ipv6 mld query-interval

Use the `ipv6 mld query-interval` Interface Configuration mode command to configure the Query interval. Use the `no` format of the command to return to default.

Syntax

ipv6 mld query-interval `seconds`
ipv6 mld query-interval

Parameters

`seconds`—Frequency, in seconds, at which MLD query messages are sent on the interface. (Range: 30–18000)

Default Configuration

125

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the frequency value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

You can execute the command before the VLAN is created.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld query-interval 3000
### 41.9 ipv6 mld query-max-response-time

Use the `ipv6 mld query-max-response-time` Interface Configuration mode command to configure the Query Maximum Response time. Use the `no` format of the command to return to default.

**Syntax**

```
ipv6 mld query-max-response-time seconds
no ipv6 mld query-max-response-time
```

**Parameter**

`seconds`—Maximum response time, in seconds, advertised in MLD queries.
(Range: 5–20)

**Default Configuration**

10

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command provides the maximum response time value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxx(config)# interface vlan 1  
switchxxxxxx(config-if)# ipv6 mld query-max-response-time 5
```

### 41.10 ipv6 mld last-member-query-count

Use the `ipv6 mld last-member-query-count` Interface Configuration mode command to configure the Last Member Query Count. This is the number of Multicast address specific queries sent before the router assumes there are no
local listeners. The Last Listener Query Count is also the number of Multicast Address and Source Specific Queries sent before the router assumes there are no listeners for a particular source.

Use the no format of the command to return to default.

**Syntax**

```
ipv6 mld last-member-query-count count
no ipv6 mld last-member-query-count
```

**Parameters**

- **count**—The number of times that group- or group-source-specific queries are sent upon receipt of a Leave message. (Range: 1–7)

**Default Configuration**

The value of the Robustness variable.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

This command provides this value if it is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxxxx(config)# interface vlan 1
switchxxxxxxx(config-if)# ipv6 mld last-member-query-count 3
```

### 41.11 ipv6 mld last-member-query-interval

Use the `ipv6 mld last-member-query-interval` interface configuration command to configure the Last Member Query Interval. Use the no format of the command to return to default.
IPv6 MLD Snooping Commands

Syntax

ipv6 mld last-member-query-interval milliseconds

no ipv6 mld last-member-query-interval

Parameter

milliseconds—Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–64512).

Default Configuration

1000

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides this value if it is not is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

You can execute the command before the VLAN is created.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 2000

41.12 ipv6 mld snooping vlan immediate-leave

Use the ipv6 mld snooping vlan immediate-leave Global Configuration mode command to enable MLD Snooping Immediate-Leave processing on a VLAN. When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients.

MLD snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface.
Use the no format of the command to return to disable MLD Snooping Immediate-Leave processing.

Syntax
ipv6 mld snooping vlan vlan-id immediate-leave
no ipv6 mld snooping vlan vlan-id immediate-leave

Parameters
vlan-id—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
You can execute the command before the VLAN is created.

Example
switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave

41.13 show ipv6 mld snooping mrouter

The show ipv6 mld snooping mrouter EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

Syntax
show ipv6 mld snooping mrouter [interface vlan-id]

Parameters
interface vlan-id—Specifies the VLAN ID.

Default Configuration
Display information for all VLANs.
Command Mode
EXEC mode

Example
The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000

switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
VLAN  Static  Dynamic  Forbidden
----  ------  ---------  ---------
1000  gi1/1/1  gi1/1/2   gi1/1/3-23

41.14 show ipv6 mld snooping interface
The show ipv6 mld snooping interface EXEC mode command displays the IPv6 MLD snooping configuration for a specific VLAN.

Syntax
show ipv6 mld snooping interface vlan-id

Parameters
vlan-id—Specifies the VLAN ID.

Default Configuration
Display information for all VLANs.

Command Mode
EXEC mode

Example
The following example displays the MLD snooping configuration for VLAN 1000.

switchxxxxxx# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping Querier is globally enabled
MLD Snooping Querier election is enabled
MLD Snooping Querier is enabled on the VLAN
MLD Snooping Querier version: 1
MLD Snooping admin: Enabled
MLD snooping oper mode: Enabled
Routers MLD version: 2
Groups that are in MLD version 1 compatibility mode:
FF12::3, FF12::8
MLD snooping robustness: admin 2  oper 2
MLD snooping query interval: admin 125 sec  oper 125 sec
MLD snooping query maximum response: admin 10 sec  oper 10 sec
MLD snooping last member query counter: admin 2  oper 2
MLD snooping last member query interval: admin 1000 msec  oper 600 msec
MLD snooping last immediate leave: enable
Automatic learning of multicast router ports is enabled

41.15  show ipv6 mld snooping groups

The show ipv6 mld snooping groups EXEC mode command displays the multicast groups learned by the MLD snooping.

Syntax

```text
show ipv6 mld snooping groups [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-address]
```

Parameters

- `vlan vlan-id`—Specifies the VLAN ID.
- `address ipv6-multicast-address`—Specifies the IPv6 multicast address.
- `source ipv6-address`—Specifies the IPv6 source address.

Command Mode

EXEC mode
Default Configuration
Display information for all VLANs and addresses defined on them.

User Guidelines
To see the full multicast address table (including static addresses), use the `show bridge multicast address-table` command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.

Note: Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list.

Example
The following example shows the output for show ipv6 mld snooping groups.

```
switchxxxxxx# show ipv6 mld snooping groups

+-------+-----------------+-----------------+-----------------+---------------+---------------+----------+
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Group Address</th>
<th>Source Address</th>
<th>Include</th>
<th>Exclude</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>----------------</td>
<td>-----------------</td>
<td>----------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>1</td>
<td>FF12::3</td>
<td>FE80::201:C9FF:FE40:8001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FF12::3</td>
<td>FE80::201:C9FF:FE40:8002</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>FF12::8</td>
<td>FE80::201:C9FF:FE40:8003</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>FF12::8</td>
<td>FE80::201:C9FF:FE40:8004</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>FF12::8</td>
<td>FE80::201:C9FF:FE40:8005</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gi1/1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MLD Reporters that are forbidden statically:

+-------+-----------------+-----------------+-------+
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Group Address</th>
<th>Source Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FF12::3</td>
<td>FE80::201:C9FF:FE40:8001</td>
<td>gi1/1/8</td>
</tr>
<tr>
<td>19</td>
<td>FF12::8</td>
<td>FE80::201:C9FF:FE40:8001</td>
<td>gi1/1/9</td>
</tr>
</tbody>
</table>
```
42.1 lACP system-priority

Use the lACP system-priority Global Configuration mode command to set the system priority. Use the no form of this command to restore the default configuration.

Syntax

```
lACP system-priority value
no lACP system-priority
```

Parameters

- **value**—Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

```
switchxxxxxx(config)# lACP system-priority 120
```

42.2 lACP port-priority

Use the lACP port-priority Interface Configuration (Ethernet) mode command to set the physical port priority. Use the no form of this command to restore the default configuration.

Syntax

```
lACP port-priority value
```

Parameters

- **value**—Specifies the port priority value.
no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1use the no form of this command65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example sets the priority of gi1/1/6.

switchxxxxxx(config)# interface gi1/1/6
switchxxxxxx(config-if)# lacp port-priority 247

42.3 lacp timeout

Use the lacp timeout Interface Configuration (Ethernet) mode command to assign an administrative LACP timeout to an interface. Use the no form of this command to restore the default configuration.

Syntax

lacp timeout {long | short}

no lacp timeout

Parameters

- long—Specifies the long timeout value.
- short—Specifies the short timeout value.

Default Configuration

The default port timeout value is Long.
**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example assigns a long administrative LACP timeout to gi1/1/6.

```plaintext
switchxxxxxx(config)# interface gi1/1/6
switchxxxxxx(config-if)# lacp timeout long
```

### 42.4 show lacp

Use the `show lacp` EXEC mode command to display LACP information for all Ethernet ports or for a specific Ethernet port.

**Syntax**

```plaintext
show lacp interface-id [parameters | statistics | protocol-state]
```

**Parameters**

- `interface-id` — Specify an interface ID. The interface ID must be an Ethernet port.
- `parameters` — Displays parameters only.
- `statistics` — Displays statistics only.
- `protocol-state` — Displays protocol state only.

**Command Mode**

EXEC mode

**Example**

The following example displays LACP information for gi1/1/1.

```plaintext
switchxxxxxx# show lacp ethernet gi1/1/1
Port gi1/1/1 LACP parameters:
   Actor
```
system priority: 1
system mac addr: 00:00:12:34:56:78
port Admin key: 30
port Oper key: 30
port Oper number: 21
port Admin priority: 1
port Oper priority: 1
port Admin timeout: LONG
port Oper timeout: LONG
LACP Activity: ACTIVE
Aggregation: AGGREGATABLE
synchronization: FALSE
collecting: FALSE
distributing: FALSE
expired: FALSE

Partner
system priority: 0
system mac addr: 00:00:00:00:00:00
port Admin key: 0
port Oper key: 0
port Oper number: 0
port Admin priority: 0
port Oper priority: 0
port Admin timeout: LONG
port Oper timeout: LONG
LACP Activity: PASSIVE
Aggregation: AGGREGATABLE
synchronization: FALSE
collecting: FALSE
distributing: FALSE
expired: FALSE

Port gi1/1/1 LACP Statistics:
LACP PDUs sent: 2
LACP PDUs received: 2

Port gi1/1/1 LACP Protocol State:
LACP State Machines:
Receive FSM: Port Disabled State
Mux FSM: Detached State
42.5 show lacp port-channel

Use the `show lacp port-channel` EXEC mode command to display LACP information for a port-channel.

**Syntax**

```
show lacp port-channel [port_channel_number]
```

**Parameters**

- **port_channel_number**—Specifies the port-channel number.

**Command Mode**

EXEC mode

**Example**

The following example displays LACP information about port-channel 1.

```
swIthxxxxx# show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet
    Actor
```

Control Variables:

- **BEGIN:** FALSE
- **LACP Enabled:** TRUE
- **Ready_N:** FALSE
- **Selected:** UNSELECTED
- **Port Moved:** FALSE
- **NNT:** FALSE
- **Port Enabled:** FALSE

Timer counters:

- **periodic tx timer:** 0
- **current while timer:** 0
- **wait while timer:** 0
### System

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Priority</td>
<td>1</td>
</tr>
<tr>
<td>MAC Address</td>
<td>000285:0E1C00</td>
</tr>
<tr>
<td>Admin Key</td>
<td>29</td>
</tr>
<tr>
<td>Oper Key</td>
<td>29</td>
</tr>
</tbody>
</table>

### Partner

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Priority</td>
<td>0</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>Oper Key</td>
<td>14</td>
</tr>
</tbody>
</table>
GARP VLAN Registration Protocol (GVRP) Commands

43.1  gvrp enable (Global)

Use the `gvrp enable` Global Configuration mode command to enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally. Use the `no` form of this command to disable GVRP on the device.

Syntax

```
gvrp enable
no gvrp enable
```

Parameters

N/A

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
switchxxxxxx(config)# gvrp enable
```

43.2  gvrp enable (Interface)

Use the `gvrp enable` Interface Configuration (Ethernet, Port-channel) mode command to enable GVRP on an interface. Use the `no` form of this command to disable GVRP on an interface.

Syntax

```
gvrp enable
```

Parameters

N/A

Default Configuration

GVRP is globally disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel)

Example

The following example enables GVRP on an interface.

```
switchxxxxxx(config-if)# gvrp enable
```
no gvrp enable

Default Configuration
GVRP is disabled on all interfaces.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
An access port does not dynamically join a VLAN because it is always a member of a single VLAN only. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN ID.

Example
The following example enables GVRP on gi1/1/6.

```
switchxxxxxx(config)# interface gi1/1/6
switchxxxxxx(config-if)# gvrp enable
```

43.3 gvrp vlan-creation-forbid
Use the `gvrp vlan-creation-forbid` Interface Configuration mode command to disable dynamic VLAN creation or modification. Use the `no` form of this command to enable dynamic VLAN creation or modification.

Syntax
```
gvrp vlan-creation-forbid
no gvrp vlan-creation-forbid
```

Default Configuration
Enabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode
Example

The following example disables dynamic VLAN creation on gi1/1/3.

```
switchxxxxxxx(config)# interface gi1/1/3
switchxxxxxxx(config-if)# gvrp vlan-creation-forbid
```

43.4  gvrp registration-forbid

Use the `gvrp registration-forbid` Interface Configuration mode command to deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port. Use the `no` form of this command to allow dynamic registration of VLANs on a port.

**Syntax**

```
gvrp registration-forbid
no gvrp registration-forbid
```

**Default Configuration**

Dynamic registration of VLANs on the port is allowed.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**Example**

The following example forbids dynamic registration of VLANs on gi1/1/2.

```
switchxxxxxxx(config)# interface gi1/1/2
switchxxxxxxx(config-if)# gvrp registration-forbid
```

43.5  clear gvrp statistics

Use the `clear gvrp statistics` Privileged EXEC mode command to clear GVRP statistical information for all interfaces or for a specific interface.
### clear gvrp statistics [interface-id]

**Syntax**

clear gvrp statistics [interface-id]

**Parameters**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Default Configuration**

All GVRP statistics are cleared.

**Command Mode**

Privileged EXEC mode

**Example**

The following example clears all GVRP statistical information on gi1/1/5.

```
switchxxxxxx# clear gvrp statistics gi1/1/5
```

### show gvrp configuration

Use the `show gvrp configuration` EXEC mode command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

**Syntax**

show gvrp configuration [interface-id | detailed]

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

All GVRP statistics are displayed for all interfaces. If detailed is not used, only present ports are displayed.
Command Mode

EXEC mode

Example

The following example displays GVRP configuration.

```
switchxxxxxx# show gvrp configuration
GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094
Port(s) GVRP-Status Regist- Dynamic          Timers(ms)
ation VLAN Creation    Join   Leave   Leave All
----    ----------- --------   -------------    ----    -----   ----------
gi1/1/1   Enabled     Forbidden   Disabled         600     200    10000

43.7 show gvrp statistics

Use the show gvrp statistics EXEC mode command to display GVRP statistics for all interfaces or for a specific interface.

Syntax

show gvrp statistics [interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP statistics are displayed.

Command Mode

EXEC mode
Example

The following example displays GVRP statistical information.

switchxxxxxx# show gvrp statistics

GVRP statistics:

Legend:

- rJE : Join Empty Received
- rEmp: Empty Received
- rLE : Leave Empty Received
- sJE : Join Empty Sent
- sEmp: Empty Sent
- sLE : Leave Empty Sent

<table>
<thead>
<tr>
<th>Port</th>
<th>rJE</th>
<th>rJIn</th>
<th>rEmp</th>
<th>rLIn</th>
<th>rLE</th>
<th>rLA</th>
<th>sJE</th>
<th>sJIn</th>
<th>sEmp</th>
<th>sLIn</th>
<th>sLE</th>
<th>sLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi1/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

43.8 show gvrp error-statistics

Use the show gvrp error-statistics EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

show gvrp error-statistics [interface-id]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
Default Configuration
All GVRP error statistics are displayed.

Command Mode
EXEC mode

Example
The following example displays GVRP error statistics.

```
switchxxxxxx# show gvrp error-statistics
GVRP Error Statistics:
------------------------
Legend:
  INVPROT : Invalid Protocol Id
  INVATYP : Invalid Attribute Type  INVALEN : Invalid Attribute Length
  INVAVAL : Invalid Attribute Value INVEVENT: Invalid Event
  Port INVPROT INVATYP INVAVAL INVALEN INVEVENT
-------- ------- ------- ------- ------- --------
  gi1/1/1      0       0       0       0       0
  gi1/1/2      0       0       0       0       0
  gi1/1/3      0       0       0       0       0
  gi1/1/4      0       0       0       0       0
  gi1/1/5      0       0       0       0       0
  gi1/1/6      0       0       0       0       0
  gi1/1/7      0       0       0       0       0
  gi1/1/8      0       0       0       0       0
```
DHCP Snooping and ARP Inspection Commands

44.1 ip dhcp snooping

Use the `ip dhcp snooping` Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the `no` form of this command to restore the default configuration.

**Syntax**

`ip dhcp snooping`

`no ip dhcp snooping`

**Parameters**

N/A

**Default Configuration**

DHCP snooping is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the `ip dhcp snooping vlan` Global Configuration mode command.

**Example**

The following example enables DHCP Snooping on the device.

```
Console(config)# ip dhcp snooping
```
44.2 ip dhcp snooping vlan

Use the ip dhcp snooping vlan Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the no form of this command to disable DHCP Snooping on a VLAN.

Syntax

ip dhcp snooping vlan vlan-id
no ip dhcp snooping vlan-id

Parameters

vlan-id—Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
Console(config)# ip dhcp snooping vlan 21
```
no ip dhcp snooping trust

Parameters
N/A

Default Configuration
The interface is untrusted.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example
The following example configures gi1/1/5 as trusted for DHCP Snooping.

```
Console(config)# interface gi1/1/5
Console(config-if)# ip dhcp snooping trust
```

44.4 ip dhcp snooping information option allowed-untrusted

Use the `ip dhcp snooping information option allowed-untrusted` Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the `no` form of this command to drop these packets from an untrusted port.

Syntax

```
ip dhcp snooping information option allowed-untrusted
no ip dhcp snooping information option allowed-untrusted
```

Parameters
N/A
**Default Configuration**

DHCP packets with option-82 information from an untrusted port are discarded.

**Command Mode**

Global Configuration mode

**Example**

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
Console(config)# ip dhcp snooping information option allowed-untrusted
```

### 44.5 ip dhcp snooping verify

Use the `ip dhcp snooping verify` Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the `no` form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

**Syntax**

```
ip dhcp snooping verify
no ip dhcp snooping verify
```

**Default Configuration**

The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

**Command Mode**

Global Configuration mode

**Example**

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
Console(config)# ip dhcp snooping verify
```
44.6 ip dhcp snooping database

Use the `ip dhcp snooping database` Global Configuration mode command to enable the DHCP Snooping binding database file. Use the `no` form of this command to delete the DHCP Snooping binding database file.

**Syntax**

`ip dhcp snooping database`
`no ip dhcp snooping database`

**Parameters**

N/A

**Default Configuration**

The DHCP Snooping binding database file is not defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

**Example**

The following example enables the DHCP Snooping binding database file.

```
Console(config)# ip dhcp snooping database
```

44.7 ip dhcp snooping database update-freq

Use the `ip dhcp snooping database update-freq` Global Configuration mode command to set the update frequency of the DHCP Snooping binding database file. Use the `no` form of this command to restore the default configuration.
DHCP Snooping and ARP Inspection Commands

44

Syntax

ip dhcp snooping database update-freq seconds
no ip dhcp snooping database update-freq

Parameters

seconds—Specifies the update frequency in seconds. (Range: 600–86400)

Default Configuration

The default update frequency value is 1200 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the DHCP Snooping binding database file update frequency to 1 hour.

Console(config)# ip dhcp snooping database update-freq 3600

44.8 ip dhcp snooping binding

Use the ip dhcp snooping binding Privileged EXEC mode command to configure the DHCP Snooping binding database and add binding entries to the database. Use the no form of this command to delete entries from the binding database.

Syntax

ip dhcp snooping binding mac-address vlan-id ip-address interface-id expiry [seconds | infinite]
no ip dhcp snooping binding mac-address vlan-id

Parameters

- mac-address— Specifies a MAC address.
- vlan-id— Specifies a VLAN number.
- ip-address— Specifies an IP address.
DHCP Snooping and ARP Inspection Commands

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

- **expiry**
  - **seconds**—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967294)
  - **infinite**—Specifies infinite lease time.

**Default Configuration**

No static binding exists.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry is displayed in the show commands as a DHCP Snooping entry.

The user cannot delete dynamic temporary entries for which the IP address is 0.0.0.0.

The user can add static entry to the DHCP Snooping database by using the command `ip source-guard binding`.

**Example**

The following example adds a binding entry to the DHCP Snooping binding database.

```
Console# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 gi1/1/5 expiry 900
```

**44.9 clear ip dhcp snooping database**

Use the `clear ip dhcp snooping database` Privileged EXEC mode command to clear the DHCP Snooping binding database.
**clear ip dhcp snooping database**

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example clears the DHCP Snooping binding database.

```
Console# clear ip dhcp snooping database
```

**show ip dhcp snooping**

Use the `show ip dhcp snooping` EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

**Syntax**

```
show ip dhcp snooping [interface-id]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode

**Example**

The following example displays the DHCP snooping configuration.

```
console# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
```
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/1</td>
<td>Yes</td>
</tr>
<tr>
<td>gi1/1/2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 44.11 show ip dhcp snooping binding

Use the `show ip dhcp snooping binding` User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

**Syntax**

```
show ip dhcp snooping binding [mac-address mac-address] [ip-address ip-address] [vlan vlan-id] [interface-id]
```

**Parameters**

- `mac-address mac-address`—Specifies a MAC address.
- `ip-address ip-address`—Specifies an IP address.
- `vlan vlan-id`—Specifies a VLAN ID.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

User EXEC mode
Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.

```
Console# show ip dhcp snooping binding

Update frequency: 1200
Total number of binding: 2

Mac Address    IP Address    Lease (sec)  Type      VLAN  Interface
--------------- ------------- ----------- --------- -------- ------------
0060.704C.73FF  10.1.8.1     7983        snooping  3       gi1/1/21
0060.704C.7BC1  10.1.8.2     92332       snooping  3       gi1/1/22
```

44.12 ip source-guard

Use the `ip source-guard` command in Configuration mode or Interface Configuration mode to enable IP Source Guard globally on a device or in Interface Configuration (Ethernet, Port-channel) mode to enable IP Source Guard on an interface.

Use the `no` form of this command to disable IP Source Guard on the device or on an interface.

Syntax

```
ip source-guard
no ip source-guard
```

Parameters

N/A

Default Configuration

IP Source Guard is disabled.

Command Mode

Configuration or Interface Configuration (Ethernet, Port-channel) mode
User Guidelines

IP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VL ANs are DHCP snooping enabled.

Example

The following example enables IP Source Guard on gi1/1/5.

```
Console(config)# interface gi1/1/5
Console(config-if)# ip source-guard
```

44.13 ip source-guard binding

Use the `ip source-guard binding` Global Configuration mode command to configure the static IP source bindings on the device. Use the `no` form of this command to delete the static bindings.

Syntax

```
ip source-guard binding mac-address vlan-id ip-address {interface-id}
no ip source-guard binding mac-address vlan-id
```

Parameters

- `mac-address`—Specifies a MAC address.
- `vlan-id`—Specifies a VLAN number.
- `ip-address`—Specifies an IP address.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode
User Guidelines

The device currently supports filtering that is based only on the source IP address. In future, the device might support filtering mode that is based on the MAC address and IP source address. Currently the MAC address field is an informative field.

Example

The following example configures the static IP source bindings.

```
Console(config)# ip source-guard binding 0060.704C.73FF 23 176.10.1.1 gi1/1/5
```

44.14 ip source-guard tcam retries-freq

Use the `ip source-guard tcam retries-freq` Global Configuration mode command to set the frequency of retries for TCAM resources for inactive IP Source Guard addresses. Use the `no` form of this command to restore the default configuration.

Syntax

```
ip source-guard tcam retries-freq {seconds | never}

no ip source-guard tcam retries-freq
```

Parameters

- `seconds`—Specifies the retries frequency in seconds. (Range: 10–600)
- `never`—Disables automatic searching for TCAM resources.

Default Configuration

The default retries frequency is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.
By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses. Use this command to change the search frequency or to disable automatic retries for TCAM space.

The `ip source-guard tcam locate` Privileged EXEC mode command manually retries locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP Source Guard addresses.

**Example**

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
Console(config)# ip source-guard tcam retries-freq 120
```

### 44.15 `ip source-guard tcam locate`

Use the `ip source-guard tcam locate` Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

**Syntax**

`ip source-guard tcam locate`

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Execute the `ip source-guard tcam retries-freq never` Global Configuration mode command to disable automatic retries for TCAM space, and then execute this
command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP source guard addresses.

**Example**

The following example manually retries to locate TCAM resources.

```console
Console# ip source-guard tcam locate
```

### 44.16 show ip source-guard configuration

Use the `show ip source-guard configuration` EXEC mode command to display the IP source guard configuration for all interfaces or for a specific interface.

**Syntax**

```
show ip source-guard configuration [interface-id]
```

**Parameters**

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode
Example

The following example displays the IP Source Guard configuration.

```
Console# show ip source-guard configuration
IP source guard is globally enabled.
Interface State
----------
gi1/1/21   Enabled

44.17 show ip source-guard status

Use the `show ip source-guard status` EXEC mode command to display the IP Source Guard status.

Syntax

```
show ip source-guard status [mac-address mac-address] [ip-address ip-address]
[vlan vlan]
[interface-id]
```

Parameters

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode
Example

The following examples display the IP Source Guard status.

Console# show ip source-guard status
IP source guard is globally disabled.

Console# show ip source-guard status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
<th>Status</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/21</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.1</td>
<td>0060.704C.73FF</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi1/1/22</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.2</td>
<td>0060.704C.7BC1</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi1/1/23</td>
<td>IP</td>
<td>Active</td>
<td>10.1.12.2</td>
<td>0060.704C.7BC3</td>
<td>4</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi1/1/24</td>
<td>IP</td>
<td>Active</td>
<td>Deny all</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/25</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.218</td>
<td>0060.704C.7BAC</td>
<td>3</td>
<td>Static</td>
</tr>
<tr>
<td>gi1/1/32</td>
<td>IP</td>
<td>Inactive</td>
<td>10.1.8.32</td>
<td>0060.704C.83FF</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi1/1/33</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/34</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1/1/35</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

44.18 show ip source-guard inactive

Use the show ip source-guard inactive EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

show ip source-guard inactive

Parameters

N/A

Command Mode

EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.
Use the `ip source-guard tcam retries-freq` Global Configuration mode command to change the retry frequency or to disable automatic retries for TCAM space.

Use the `ip source-guard tcam locate` Privileged EXEC mode command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

This command displays the inactive IP source guard addresses.

**Example**

The following example displays the IP source guard inactive addresses.

```
Console# show ip source-guard inactive

TBD: TCAM resources search frequency: 10 minutes

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/32</td>
<td>IP</td>
<td>10.1.8.32</td>
<td>3</td>
<td>DHCP</td>
<td>Resource Problem</td>
</tr>
<tr>
<td>gi1/1/33</td>
<td>IP</td>
<td>10.1.8.32</td>
<td>3</td>
<td>DHCP</td>
<td>Trust port</td>
</tr>
<tr>
<td>gi1/1/34</td>
<td>I</td>
<td>10.1.8.32</td>
<td>3</td>
<td>DHCP</td>
<td>No snooping</td>
</tr>
</tbody>
</table>
```

**44.19 show ip source-guard statistics**

Use the `show ip source-guard statistics` EXEC mode command to display the Source Guard dynamic information (permitted stations).

**Syntax**

```
show ip source-guard statistics [vlan vlan-id]
```

**Parameters**

- **vlan-id**—Display the statistics on this VLAN.

**Command Mode**

EXEC mode

**Example**

```
console#show ip source-guard statistics
```
### 44.20  **ip arp inspection**

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

**Syntax**

- `ip arp inspection`  
- `no ip arp inspection`

**Parameters**

N/A

**Default Configuration**

ARP inspection is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

**Example**

The following example enables ARP inspection on the device.

```
Console(config)# ip arp inspection
```
### 44.21 ip arp inspection vlan

Use the `ip arp inspection vlan` Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the `no` form of this command to disable ARP inspection on a VLAN.

**Syntax**

```
ip arp inspection vlan vlan-id
no ip arp inspection vlan vlan-id
```

**Parameters**

- `vlan-id`—Specifies the VLAN ID.

**Default Configuration**

DHCP Snooping based ARP inspection on a VLAN is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the `ip arp inspection list assign` Global Configuration mode command to enable static ARP inspection.

**Example**

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
Console(config)# ip arp inspection vlan 23
```

### 44.22 ip arp inspection trust

Use the `ip arp inspection trust` Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the `no` form of this command to restore the default configuration.
**Syntax**

ip arp inspection trust  
no ip arp inspection trust

**Parameters**

N/A

**Default Configuration**

The interface is untrusted.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the `ip arp inspection log-buffer vlan` Global Configuration mode command.

**Example**

The following example configures gi1/1/3 as a trusted interface.

```
Console(config)# interface gi1/1/3
Console(config-if)# ip arp inspection trust
```

**44.23  ip arp inspection validate**

Use the `ip arp inspection validate` Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the `no` form of this command to restore the default configuration.
Syntax

ip arp inspection validate
no ip arp inspection validate

Parameters

N/A

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.

- **IP addresses**: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

---

Console(config)# ip arp inspection validate

---

44.24  ip arp inspection list create

Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.
Syntax

ip arp inspection list create name
no ip arp inspection list create name

Parameters

name—Specifies the static ARP binding list name. (Length: 1–32 characters)

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip arp inspection list assign` command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list ‘servers’ and enters the ARP list configuration mode.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)#
```

44.25  ip mac

Use the `ip mac` ARP-list Configuration mode command to create a static ARP binding. Use the `no` form of this command to delete a static ARP binding.

Syntax

ip ip-address mac mac-address
no ip ip-address mac mac-address

Parameters

- ip-address—Specifies the IP address to be entered to the list.
- mac-address—Specifies the MAC address associated with the IP address.
Default Configuration
No static ARP binding is defined.

Command Mode
ARP-list Configuration mode

Example
The following example creates a static ARP binding.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
Console(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

44.26 ip arp inspection list assign

Use the `ip arp inspection list assign` Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the `no` form of this command to delete the assignment.

Syntax
```
ip arp inspection list assign vlan-id name
no ip arp inspection list assign vlan-id
```

Parameters
- **vlan-id**—Specifies the VLAN ID.
- **name**—Specifies the static ARP binding list name.

Default Configuration
No static ARP binding list assignment exists.

Command Mode
Global Configuration mode
Example

The following example assigns the static ARP binding list Servers to VLAN 37.

```
Console(config)# ip arp inspection list assign 37 servers
```

### 44.27 ip arp inspection logging interval

Use the `ip arp inspection logging interval` Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
ip arp inspection logging interval {seconds / infinite}
no ip arp inspection logging interval
```

**Parameters**

- **seconds**—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- **infinite**—Specifies that SYSLOG messages are not generated.

**Default Configuration**

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

**Command Mode**

Global Configuration mode

**Example**

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
Console(config)# ip arp inspection logging interval 60
```
44.28 show ip arp inspection

Use the `show ip arp inspection` EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

**Syntax**

`show ip arp inspection [interface-id]`

**Parameters**

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode

**Example**

The following example displays the ARP inspection configuration.

```
console# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds

Interface  Trusted
----------- -----------
gi1/1/1      Yes
gi1/1/2      Yes
```

44.29 show ip arp inspection list

Use the `show ip arp inspection list` Privileged EXEC mode command to display the static ARP binding list.

**Syntax**

`show ip arp inspection list`
Parameters
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the static ARP binding list.

```
Console# show ip arp inspection list
List name: servers
Assigned to VLANs: 1,2
IP  ARP
---  -------
172.16.1.1  0060.704C.7322
172.16.1.2  0060.704C.7322
```

44.30  show ip arp inspection statistics

Use the `show ip arp inspection statistics` EXEC command to display Statistics For The Following Types Of Packets That Have Been Processed By This Feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax
```
show ip arp inspection statistics [vlan vlan-id]
```

Parameters
`vlan-id`—Specifies VLAN ID.

Command Mode
EXEC mode

User Guidelines
To clear ARP Inspection counters use the `clear ip arp inspection statistics` CLI command. Counters values are kept when disabling the ARP Inspection feature.
Example

```
console# show ip arp inspection statistics

Vlan  Forwarded Packets  Dropped Packets  IP/MAC Failures

---  -------------------  -------------------  -------------------
2    1500000  80
```

44.31  clear ip arp inspection statistics

Use the `clear ip arp inspection statistics` Privileged EXEC mode command to clear ARP Inspection statistics globally.

**Syntax**

```
clear ip arp inspection statistics [vlan vlan-id]
```

**Parameters**

- `vlan-id`—Specifies VLAN ID

**Command Mode**

Privileged EXEC mode

**Example**

```
console# clear ip arp inspection statistics
```
45.1 ip address

Use the `ip address` Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the `no` form of this command to remove an IP address definition.

**Syntax**

If the product is in router mode (Layer 3).

\[
\text{ip address ip-address } \{mask \mid \text{prefix-length}\}
\]

\[
\text{no ip address } [\text{ip-address}]
\]

If the product is in switch mode (Layer 2).

\[
\text{ip address ip-address } \{mask \mid \text{prefix-length}\} [\text{default-gateway ip-address}]
\]

\[
\text{no ip address } [\text{ip-address}]
\]

\[
\text{no ip address }
\]

**Parameters**

- `ip-address`—Specifies the IP address.
- `mask`—Specifies the network mask of the IP address.
- `prefix-length`—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- `default-gateway ip-address`—Specifies the default gateway IP address.

**Default Configuration**

No IP address is defined for interfaces.

**Command Mode**

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).
User Guidelines

Defining a static IP address on an interface implicitly removes the DHCP client configuration on the interface.

If the device is in router mode, it supports multiple IP addresses. See Router Resources Commands

The IP addresses must be from different IP subnets. When adding an IP address from a subnet that already exists in the list, the new IP address replaces the existing IP address from that subnet.

If the IP address is configured in Interface context, the IP address is bound to the interface in that context.

If a static IP address is already defined, the user must do no IP address in the relevant interface context before changing the IP address.

If a dynamic IP address is already defined, the user must do no ip address in the relevant interface context before configuring another dynamic IP address.

The Interface context may be a port, LAG or VLAN, depending on support that is defined for the product.

If a configured Ip address overlaps another configured one a warning message is displayed. For example:

Example

Example 1. The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

Example 3. The following example configures 3 overlapped IP addresses.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 1.1.1.1 255.0.0.0
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ip address 1.2.1.1 255.255.0.0
```
This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you sure? [Y/N]Y

exit

interface vlan 3

ip address 1.3.1.1 255.255.0.0

This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you sure? [Y/N]Y

exit

### 45.2 ip address dhcp

Use the `ip address dhcp` Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the `no` form of this command to release an acquired IP address.

**Syntax**

```
ip address dhcp
no ip address dhcp
```

**Parameters**

N/A

**Command Mode**

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

**User Guidelines**

This command enables any interface to dynamically learn its IP address by using the DHCP protocol.

DHCP client configuration on an interface implicitly removes the static IP address configuration on the interface.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.
The **no ip address dhcp** command releases any IP address that was acquired, and sends a DHCPRELEASE message.

**Example**
The following example acquires an IP address for gi1/1/16 from DHCP.

```
switchxxxxxx(config)# interface gi1/1/16
switchxxxxxx(config-if)# ip address dhcp
```

### 45.3 renew dhcp
Use the **renew dhcp** Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

**Syntax**

```
renew dhcp interface-id [force-autoconfig]
```

**Parameters**

- **interface-id**—Only required in routing mode (Layer 3). Specifies an interface ID (Ethernet port, Port-channel or VLAN).
- **force-autoconfig** - If the DHCP server holds a DHCP option 67 record for the assigned IP address, the record overwrites the existing device configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Note the following:

- When the device is in Layer 2 (switch mode), interface-id is not required.
- This command does not enable DHCP on an interface. If DHCP is not enabled on the requested interface, the command returns an error message.
- If DHCP is enabled on the interface and an IP address was already acquired, the command tries to renew that IP address.
If DHCP is enabled on the interface and an IP address has not yet been acquired, the command initiates a DHCP request.

**Example**

The following example renews an IP address that was acquired from a DHCP server for VLAN 19. This assumes that the device is in Layer 3.

```
switchxxxxxx# renew dhcp vlan 19
```

### 45.4 ip default-gateway

The `ip default-gateway` Global Configuration mode command defines a default gateway (device). Use the `no` form of this command to restore the default configuration.

**Syntax**

```
ip default-gateway ip-address
no ip default-gateway
```

**Parameters**

- `ip-address`—Specifies the default gateway IP address.

**Command Mode**

Global Configuration mode

**Default Configuration**

No default gateway is defined.

**Example**

The following example defines default gateway 192.168.1.1.

```
switchxxxxxx(config)# ip default-gateway 192.168.1.1
```
45.5 show ip interface

Use the show ip interface EXEC mode command to display the usability status of configured IP interfaces.

Syntax

show ip interface [interface-id]

Parameters

interface-id—Specifies an interface ID on which IP addresses are defined.

Default Configuration

All IP addresses.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays the configured IP interfaces and their types when the device is in Router mode.

```
switchxxxxxx# show ip interface
IP Address       I/F     I/F Status  Type   Directed   Precedence Status
admin/oper        Broadcast
-------------    ------  ----------- ------- --------   ---------- -------
10.5.234.232/24  vlan 1  UP/UP       Static  disable    No         Valid
10.5.234.202/24  vlan 4  UP/DOWN     Static  disable    No         Valid
```

Example 2 - The following example displays the configured IP interfaces and their types when the device is in Router mode.

```
switchxxxxxx# show ip interface vlan1
IP Address       I/F     I/F Status  Type   Directed   Precedence Status
admin/oper        Broadcast
-------------    ------  ----------- ------- --------   ---------- -------
10.5.234.232/24  vlan 1  UP/UP       Static  disable    No         Valid
10.5.234.202/24  vlan 4  UP/DOWN     Static  disable    No         Valid
```
Example 3 - The following example displays the configured IP interfaces and their types when the device is in Switch mode.

switchxxxxxx# show ip interface

<table>
<thead>
<tr>
<th>Gateway IP Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.227.97</td>
<td>dhcp</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>I/F</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.227.101/27</td>
<td>vlan 1</td>
<td>DHCP</td>
<td>Valid</td>
</tr>
</tbody>
</table>

45.6  arp

Use the `arp` Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the `no` form of this command to remove an entry from the ARP cache.

Syntax

```
arp ip-address mac-address [interface-id]
no arp ip-address
```

Parameters

- `ip-address`—IP address or IP alias to map to the specified MAC address.
- `mac-address`—MAC address to map to the specified IP address or IP alias.
- `interface-id`—Address pair is added for specified interface that can be Ethernet port, Port-channel or VLAN.

Command Mode

Global Configuration mode
Default Configuration

No permanent entry is defined.
If no interface ID is entered, address pair is relevant to all interfaces.

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
switchxxxxxx(config)# arp 198.133.219.232 00:00:0c:40:0f:bc gi1/1/6
```

45.7  arp timeout (Global)

Use the `arp timeout` Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the `no` form of this command to restore the default configuration.

Syntax

```
arp timeout seconds
no arp timeout
```

Parameters

- `seconds`—Specifies the time interval (in seconds) during which an entry remains in the ARP cache.
  (Range: 1–40000000)

Default Configuration

The default ARP timeout is 60000 seconds in Router mode, and 300 seconds in Switch mode.

Command Mode

Global Configuration mode
Example
The following example configures the ARP timeout to 12000 seconds.

```
switchxxxxxx(config)# arp timeout 12000
```

45.8 ip arp proxy disable
Use the `ip arp proxy disable` Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the `no` form of this command to re-enable proxy ARP.

Syntax
```
ip arp proxy disable
no ip arp proxy disable
```

Parameters
N/A

Default
Enabled by default.

Command Mode
Global Configuration mode

User Guidelines
This command overrides any proxy ARP interface configuration. To use this command, you must put the switch into routing mode using `set system`.

Example
The following example globally disables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config)# ip arp proxy disable
```
45.9 ip proxy-arp

Use the `ip proxy-arp` Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the `no` form of this command disable it.

**Syntax**

`ip proxy-arp`

`no ip proxy-arp`

**Default Configuration**

ARP Proxy is disabled.

**Command Mode**

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

**User Guidelines**

This configuration can be applied only if at least one IP address is defined on a specific interface. To use this command, you must put the switch into routing mode using `set system`.

**Example**

The following example enables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config-if)# ip proxy-arp
```

45.10 clear arp-cache

Use the `clear arp-cache` Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

**Syntax**

`clear arp-cache`

**Command Mode**

Privileged EXEC mode
Example

The following example deletes all dynamic entries from the ARP cache.

```
switchxxxxxx# clear arp-cache
```

45.11 show arp

Use the `show arp` Privileged EXEC mode command to display entries in the ARP table.

**Syntax**

```
show arp [ip-address ip-address] [mac-address mac-address] [interface-id]
```

**Parameters**

- `ip-address ip-address`—Specifies the IP address.
- `mac-address mac-address`—Specifies the MAC address.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.
Example

The following example displays entries in the ARP table.

```
switchxxxxxx# show arp
ARP timeout: 80000 Seconds
VLAN Interface IP Address   HW Address     Status
--------- -------- --------- ------------- --------
VLAN 1   gi1/1/1  10.7.1.102 00:10:B5:04:DB:4B Dynamic
VLAN 1   gi1/1/2  10.7.1.135 00:50:22:00:2A:A4  Static
```

45.12 `show arp configuration`

Use the `show arp configuration` privileged EXEC command to display the global and interface configuration of the ARP protocol.

Syntax

`show arp configuration`

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show arp configuration
Global configuration:
   ARP Proxy: enabled
   ARP timeout: 80000 Seconds
Interface configuration:
g2:
   ARP Proxy: disabled
   ARP timeout:60000 Seconds
VLAN 1:
```
ARP Proxy: enabled
ARP timeout: 70000 Seconds

VLAN 2:
ARP Proxy: enabled
ARP timeout: 80000 Second (Global)

### 45.13 interface ip

Use the `interface ip` Global Configuration mode command to enter the IP Interface Configuration mode.

This command can only be used when the device is in Router mode.

**Syntax**

`interface ip-address`

**Parameters**

`ip-address`—Specifies one of the IP addresses of the device.

**Command Mode**

Global Configuration mode

**User Guidelines**

To use this command, you must put the switch into routing mode using `set system`.

**Example**

The following example enters the IP interface configuration mode.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)#
```

### 45.14 ip helper-address

Use the `ip helper-address` Global Configuration mode command to enable the forwarding of UDP Broadcast packets received on an interface to a specific
(helper) address. Use the no form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

This command can only be used when the device is in Router mode.

Syntax

```
ip helper-address {ip-interface | all} address [udp-port-list]
no ip helper-address {ip-interface | all} address
```

Parameters

- **ip-interface**—Specifies the IP interface.
- **all**—Specifies all IP interfaces.
- **address**—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- **udp-port-list**—Specifies the destination UDP port number to which to forward Broadcast packets. (Range: 1–65535). This can be a list of port numbers separated by spaces.

Default Configuration

Forwarding of UDP Broadcast packets received on an interface to a specific (helper) address is disabled.

If **udp-port-list** is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

To use this command, you must put the switch into routing mode using `set system`.

This command forwards specific UDP Broadcast packets from one interface to another, by specifying a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

**Example**

The following example enables the forwarding of UDP Broadcast packets received on all interfaces to the UDP ports of a destination IP address and UDP port 1 and 2.

```
switchxxxxx(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

**45.15 show ip helper-address**

Use the **show ip helper-address** Privileged EXEC mode command to display the IP helper addresses configuration on the system.

This command can only be used when the device is in Router mode.

**Syntax**

```
show ip helper-address
```

**Parameters**

This command has no arguments or key words.

**Command Mode**

Privileged EXEC mode
User Guidelines
To use this command, you must put the switch into routing mode using \texttt{set system}.

Example
The following example displays the IP helper addresses configuration on the system.

\begin{verbatim}
switchxxxxxx# show ip helper-address
Interface       Helper Address       UDP Ports
--------------- -------------- ------------------------
192.168.1.1      172.16.8.8          37, 42, 49, 53, 137, 138
192.168.2.1      172.16.9.9          37, 49
\end{verbatim}

45.16 \texttt{show ip dhcp client interface}

Use the \texttt{show ip dhcp client interface} command in User EXEC or Privileged EXEC mode to display DHCP client interface information.

Syntax
\texttt{show ip dhcp client interface [interface-id]}

Parameters
\texttt{interface-id}— Interface identifier.

Command Mode
User EXEC
Privileged EXEC

User Guidelines
If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example
The following is sample output of the \texttt{show ip dhcp client interface} command:
show ip dhcp client interface

VLAN 100 is in client mode
  Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
  Default Gateway: 170.10.100.1
  DNS Servers: 115.1.1.1, 87.12.34.20
  DNS Domain Search List: company.com
  Host Name: switch_floor7
  Configuration Server Addresses: 192.1.1.1 202.1.1.1
  Configuration Path Name: qqq/config/aaa_config.dat
  POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00

VLAN 1200 is in client mode
  Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
  Default Gateway: 180.10.100.1
  DNS Servers: 115.1.1.1, 87.12.34.20
  DNS Domain Search List: company.com
  Host Name: switch_floor7
  Configuration Server Addresses: configuration.company.com
  Configuration Path Name: qqq/config/aaa_config.dat
  POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
IPv6 Router Commands

46.1 clear ipv6 neighbors

Use the clear ipv6 neighbors command in privileged EXEC mode to delete all entries in the IPv6 neighbor discovery cache, except static entries.

Syntax

clear ipv6 neighbors

Parameters

N/A

Command Mode

Privileged EXEC

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
switchxxxx#clear ipv6 neighbors
```

46.2 clear ipv6 prefix-list

Use the clear ipv6 prefix-list command in privileged EXEC mode to reset the hit count of the IPv6 prefix list entries.

Syntax

```
clear ipv6 prefix-list [prefix-list-name [ipv6-prefix/ prefix-length]]
```
Parameters

- **prefix-list-name**—The name of the prefix list from which the hit count is to be cleared.
- **ipv6-prefix**—The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

The hit count is automatically cleared for all IPv6 prefix lists.

Command Mode

Privileged EXEC

User Guidelines

The hit count is a value indicating the number of matches to a specific prefix list entry.

Example

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35:

```
switchxxx#clear ipv6 prefix-list first_list 2001:0DB8::/35
```

46.3 ipv6 address

Use the **ipv6 address** command in Interface Configuration mode to configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface. To remove the address from the interface, use the **no** form of this command.

Syntax

```
ipv6 address ipv6-address/prefix-length
```
no ipv6 address [ipv6-address prefix-length]

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **prefix-length**—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration

User Guidelines

The `ipv6 address` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no IPv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example defines the IPv6 global address 2001:DB8:2222:7272::72 on vlan 100:

```
interface vlan 100
  ipv6 address 2001:DB8:2222:7272::72/64
exit
```

**ipv6 address anycast**

Use the `ipv6 address anycast` command in Interface Configuration mode to configure an IPv6 Anycast address and enable IPv6 processing on an interface.
To remove the address from the interface, use the no form of this command.

**Syntax**

```
ipv6 address ipv6-prefix/prefix-length anycast
no ipv6 address [ipv6-prefix/prefix-length anycast]
```

**Parameters**

- `ipv6-address`—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `prefix-length`—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

**Default Configuration**

No IP address is defined for the interface.

**Command Mode**

Interface Configuration

**User Guidelines**

An Anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface—as defined by the routing protocols in use—identified by the Anycast address. Anycast addresses are syntactically indistinguishable from Unicast addresses because Anycast addresses are allocated from the Unicast address space. Nodes to which the Anycast address is assigned must be explicitly configured to recognize that the address is an Anycast address.

Anycast addresses can be used only by a router, not a host, and Anycast addresses must not be used as the source address of an IPv6 packet.

The subnet router Anycast address has a prefix concatenated by a series of zeros (the interface ID). The subnet router Anycast address can be used to reach a router on the link that is identified by the prefix in the subnet router Anycast address.

The `ipv6 address anycast` command cannot be applied to define an IPv6 address on an ISATAP interface.
Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

**Example**

The following example enables IPv6 processing on the interface, assigns the prefix 2001:0DB8:1:1::/64 to the interface, and configures the IPv6 Anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
interface vlan 1
  ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
exit
```

### 46.5 ipv6 address autoconfig

Use the `ipv6 address autoconfig` command in Interface Configuration mode to enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.

To remove the address from the interface, use the `no` form of this command.

**Syntax**

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

**Parameters**

N/A.

**Default Configuration**

Stateless Auto configuration is disabled.

**Command Mode**

Interface Configuration mode.
User Guidelines

This command enables IPv6 on an interface (if it was disabled) and causes the switch to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the eui-64 based addresses to the interface.

Stateless auto configuration is applied only when IPv6 Forwarding is disabled.

When IPv6 forwarding is changed from disabled to enabled, and stateless auto configuration is enabled the switch stops stateless auto configuration and removes all stateless auto configured ipv6 addresses from all interfaces.

When IPv6 forwarding is changed from enabled to disabled and stateless auto configuration is enabled the switch resumes stateless auto configuration.

Using the no ipv6 address autoconfig command to disable stateless auto configuration and to remove all stateless auto configured IPv6 addresses from an interface.

Example

The following example assigns the IPv6 address automatically:

```
interface vlan 100
  ipv6 address autoconfig
exit
```

46.6 ipv6 address eui-64

Use the ipv6 address eui-64 command in Interface Configuration mode to configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address.

To remove the address from the interface, use the no form of this command.

Syntax

```
ipv6 address ipv6-prefix/prefix-length eui-64
no ipv6 address [ipv6-prefix/prefix-length]
```

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length**—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

**Default Configuration**

No IP address is defined for the interface.

**Command Mode**

Interface Configuration

**User Guidelines**

If the value specified for the **prefix-length** argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

If the switch detects another host using one of its IPv6 addresses, it adds the IPv6 address and displays an error message on the console.

Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

**Example**

The following example enables IPv6 processing on VLAN 1, configures IPv6 global address 2001:0DB8:0:1::/64 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
interface vlan 1
  ipv6 address 2001:0DB8:0:1::/64 eui-64
exit
```

### 46.7 **ipv6 address link-local**

Use the **ipv6 address link-local** command in Interface Configuration mode to configure an IPv6 link local address for an interface and enable IPv6 processing on the interface.

To remove the manually configured link local address from the interface, use the **no** form of this command.
Syntax
ipv6 address ipv6-prefix link-local
no ipv6 address [link-local]

Parameters
- ipv6-address—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

Default Configuration
The default Link-local address is defined.

Command Mode
Interface Configuration

User Guidelines
The switch automatically generates a link local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link local address to be used by an interface, use the ipv6 address link-local command.

The ipv6 address link-local command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the no IPv6 address command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example
The following example enables IPv6 processing on VLAN 1 and configures FE80::260:3EFF:FE11:6770 as the link local address for VLAN 1:

```
interface vlan 1
  ipv6 address FE80::260:3EFF:FE11:6770 link-local
  exit
```
46.8 ipv6 default-gateway

Use the ipv6 default-gateway Global Configuration mode command to define an IPv6 default gateway.

To remove the default gateway, use the no form of this command.

Syntax

ipv6 default-gateway ipv6-address | interface-id
no ipv6 default-gateway ipv6-address | interface-id

Parameters

- ipv6-address—Specifies the IPv6 address of the next hop that can be used to reach a network.
- interface-id—Specifies the Interface Identifier of the outgoing interface that can be used to reach a network.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

The command is an alias of the ipv6 route command with the predefined (default) route:

ipv6 route ::/0 ipv6-address | interface-id

See the definition of the ipv6 route command for details.

Example

The following example configures a default gateway:

switchxxxxxxx(config)# ipv6 default-gateway fe80::abcd%vlan1

46.9 ipv6 enable

Use the ipv6 enable command in Interface Configuration mode to enable IPv6 processing on an interface.
To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the no form of this command.

**Syntax**

```
ipv6 enable
no ipv6 enable
```

**Parameters**

N/A.

**Default Configuration**

IPv6 addressing is disabled.

**Command Mode**

Interface Configuration

**User Guidelines**

This command automatically configures an IPv6 link-local Unicast address on the interface while also enabling the interface for IPv6 processing. The `no ipv6 enable` command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

**Example**

The following example enables VLAN 1 for the IPv6 addressing mode.

```
interface vlan 1
  ipv6 enable
exit
```

### 46.10 ipv6 hop-limit

Use the `ipv6 hop-limit` command in Global Configuration mode to configure the maximum number of hops used in all IPv6 packets that are originated by the router.

To return the hop limit to its default value, use the no form of this command.
**IPv6 hop-limit**

Syntax

ipv6 hop-limit value

no ipv6 hop-limit

Parameters

value—Maximum number of hops. The acceptable range is from 1 to 255.

Default Configuration

The default is 64 hops.

Command Mode

Global Configuration

Example

The following example configures a maximum number of 15 hops for all IPv6 packets that are originated from the router:

```
switchxxxxxx(config)#ipv6 hop-limit 15
```

---

**46.11 ipv6 icmp error-interval**

Use the `ipv6 icmp error-interval` command in Global Configuration mode to configure the interval and bucket size for IPv6 ICMP error messages. To return the interval to its default setting, use the `no` form of this command.

Syntax

ipv6 icmp error-interval milliseconds [bucketsize]

no ipv6 icmp error-interval

Parameters

- milliseconds—Time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0 to 2147483647. A value of 0 disables ICMP rate limiting.

- bucketsize—Maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200.
Default Configuration

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second.

Command Mode

Global Configuration mode

User Guidelines

Use this command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The `milliseconds` argument specifies the time interval between tokens arriving in the bucket. The optional `bucketsize` argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the `bucketsize` is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Average Packets Per Second = \((1000/ \text{milliseconds}) \times \text{bucketsize}\).

To disable ICMP rate limiting, set the `milliseconds` argument to zero.

Example

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
switchxxxxxx(config)#ipv6 icmp error-interval 50 20
```

### 46.12  ipv6 link-local default zone

Use the `ipv6 link-local default zone` command to configure an interface to egress a link local packet without a specified interface or with the default zone 0.

Use the `no` form of this command to return the default link local interface to the default value.

**Syntax**

```
ipv6 link-local default zone interface-id
```
no ipv6 link-local default zone

Parameters

interface-id—Specifies the interface that is used as the egress interface for packets sent without a specified IPv6Z interface identifier or with the default 0 identifier.

Default

By default, link local default zone is disabled.

Command Mode

Global Configuration mode

Example

The following example defines VLAN 1 as a default zone:

```
switchxxxxxx(config)#ipv6 link-local default zone vlan1
```

### 46.13 ipv6 mld version

Use the ipv6 mld version Interface Configuration mode command to specify the version of the MLD.

To return to the default version, use the no form of this command.

Syntax

ipv6 mld version 1/2

no ipv6 mld version

Parameters

- 1—Specifies MLD version 1.
- 2—Specifies MLD version 2.

Default Configuration

MLD version 1.
Command Mode
Interface Configuration

Example
The following example defines MLDv2 on VLAN 1:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld version 2
```

46.14  ipv6 nd advertisement-interval
Use the `ipv6 nd advertisement-interval` in Interface Configuration mode to configure the advertisement interval option in router advertisements (RAs).
To reset the interval to the default value, use the `no` form of this command.

Syntax
ipv6 nd advertisement-interval
no ipv6 nd advertisement-interval

Parameters
N/A.

Default Configuration
Advertisement interval option is not sent.

Command Mode
Interface Configuration

User Guidelines
Use the `ipv6 nd advertisement-interval` command to indicate to a visiting mobile node the interval at which that node may expect to receive RAs. The node may use this information in its movement detection algorithm.
Example
The following example enables the advertisement interval option to be sent in RAs:

```
interface vlan 1
  ipv6 nd advertisement-interval
exit
```

46.15 ipv6 nd dad attempts

Use the `ipv6 nd dad attempts` command in Interface Configuration mode to configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface.

To return the number of messages to the default value, use the `no` form of this command.

Syntax

```
ipv6 nd dad attempts value
no ipv6 nd dad attempts
```

Parameters

`value`—The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Default Configuration

```
1
```

Command Mode

Interface Configuration

User Guidelines

Duplicate address detection verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed).
Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of Unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 4862, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface, while duplicate address detection is performed on a tentative Unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 4861, Neighbor Discovery for IPv6), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the `ipv6 nd ns-interval` command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the Unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

An interface returning to administratively up, restarts duplicate address detection for all of the Unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error SYSLOG message is issued.

If the duplicate address is a global address of the interface, the address is not used and an error SYSLOG message is issued.

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).
**Note.** Since DAD is not supported on NBMA interfaces the command is allowed but does not impact on an IPv6 tunnel interface of the ISATAP type it does not impact. The configuration is saved and will impacted when the interface type is changed on another type on which DAD is supported (for example, to the IPv6 manual tunnel).

**Example**

The following example configures five consecutive neighbor solicitation messages to be sent on VLAN 1 while duplicate address detection is being performed on the tentative Unicast IPv6 address of the interface. The example also disables duplicate address detection processing on VLAN 2.

```plaintext
interface vlan 1
  ipv6 nd dad attempts 5
exit
interface vlan 2
  ipv6 nd dad attempts 0
exit
```

### 46.16  ipv6 nd hop-limit

Use the `ipv6 nd hop-limit` command in Global Configuration mode to configure the maximum number of hops used in router advertisements.

To return the hop limit to its default value, use the `no` form of this command.

**Syntax**

```
ipv6 nd hop-limit value
no ipv6 nd hop-limit
```

**Parameters**

- `value`—Maximum number of hops. The acceptable range is from 1 to 255.

**Default Configuration**

The default value is defined by the `ipv6 hop-limit` command, or is set to 64 hops, if the command was not configured.
**Command Mode**

Interface Configuration

**User Guidelines**

Use this command if you want to change the default value. The default value is defined by the `ipv6 hop-limit` command.

**Example**

The following example configures a maximum number of 15 hops for router advertisements on VLAN 2:

```
interface vlan 2
    ipv6 nd hop-limit 15
exit
```

### 46.17 ipv6 nd managed-config-flag

Use the `ipv6 nd managed-config-flag` command in Interface Configuration mode to set the “managed address configuration flag” in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the `no` form of this command.

**Syntax**

- `ipv6 nd managed-config-flag`
- `no ipv6 nd managed-config-flag`

**Parameters**

N/A.

**Default Configuration**

The “managed address configuration flag” flag is not set in IPv6 router advertisements.

**Command Mode**

Interface Configuration
User Guidelines

Setting the Managed Address Configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If this flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses, and if it is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Example

The following example configures the Managed Address Configuration flag in IPv6 router advertisements on VLAN 1:

```
interface vlan 1
  ipv6 nd managed-config-flag
exit
```

46.18  ipv6 nd ns-interval

Use the `ipv6 nd ns-interval` command in Interface Configuration mode to configure the interval between IPv6 neighbor solicitation retransmissions on an interface.

To restore the default interval, use the `no` form of this command.

Syntax

```
ipv6 nd ns-interval milliseconds
no ipv6 nd ns-interval
```

Parameters

- `milliseconds`—Interval between IPv6 neighbor solicit transmissions. The acceptable range is from 1000 to 3600000 milliseconds.

Default Configuration

0 seconds (unspecified) is advertised in router advertisements and the value 1000 milliseconds is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration
**User Guidelines**

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a non-default value is configured, the configured time is both advertised and used by the router itself.

**Example**

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for VLAN 1:

```plaintext
interface vlan 1
  ipv6 nd ns-interval 9000
exit
```

### 46.19 ipv6 nd other-config-flag

Use the `ipv6 nd other-config-flag` command in Interface Configuration mode to set the Other Stateful configuration flag in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the `no` form of this command.

**Syntax**

- `ipv6 nd other-config-flag`
- `no ipv6 nd other-config-flag`

**Parameters**

N/A.

**Default Configuration**

The Other Stateful configuration flag is not set in IPv6 router advertisements.

**Command Mode**

Interface Configuration
User Guidelines

The setting of the Other Stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note. If the Managed Address Configuration flag is set using the `ipv6 nd managed-config-flag` command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the Other Stateful configuration flag.

Example

The following example configures the Other Stateful configuration flag in IPv6 router advertisements on VLAN 1:

```
interface vlan 1
  ipv6 nd other-config-flag
exit
```

46.20 ipv6 nd prefix

Use the `ipv6 nd prefix` command in Interface Configuration mode to configure which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements.

To remove the prefixes, use the `no` form of this command.

Syntax

```
ipv6 nd prefix {ipv6-prefix/prefix-length | default} [no-advertise | {[valid-lifetime preferred-lifetime] [no-autoconfig] [off-link | no-onlink]}]
```

```
no ipv6 nd prefix {ipv6-prefix/prefix-length | default}
```

Parameters

- `ipv6-prefix`—IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC4293, where the address is specified in hexadecimal using 16-bit values between colons.

- `/prefix-length`—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the
prefix (the network portion of the address). A slash mark must precede the decimal value.

- **default**—Default values used for automatic advertised prefixes configured as addresses on the interface using the `ipv6 address` command.

- **no-advertise**—Prefix is not advertised.

- **valid-lifetime**—Remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. A value of 4,294,967,295 represents infinity. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

- **preferred-lifetime**—Remaining length of time, in seconds, that this prefix will continue to be preferred, i.e., time until deprecation. A value of 4,294,967,295 represents infinity. The address generated from a deprecated prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The `preferred-lifetime` must not be larger than the `valid-lifetime`.

- **no-autoconfig**—Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The prefix will be advertised with the A-bit clear.

- **off-link**—Configures the specified prefix as off-link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured using the `ipv6 address` command), then it will be removed.

- **no-onlink**—Configures the specified prefix as not on-link. The prefix will be advertised with the L-bit clear.

**Default Configuration**

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Note that by default:

- All prefixes are inserted in the routing table as connected prefixes.
- All prefixes are advertised as on-link (for example, the L-bit is set in the advertisement)
- All prefixes are advertised as an auto-configuration prefix (for example, the A-bit is set in the advertisement)

**Command Mode**

**Interface Configuration**

**User Guidelines**

This command enables control over the individual parameters per prefix, including whether the prefix should be advertised.

Use the `ipv6 nd prefix ipv6-prefix/prefix-length` command to add the prefix to the Prefix table.

Use the `no ipv6 nd prefix ipv6-prefix/prefix-length` command to remove the prefix from the Prefix table.

Use the `no ipv6 nd prefix` command without the `ipv6-prefix/prefix-length` argument to remove all prefixes from the Prefix Table.

**Note.** The `no ipv6 nd prefix` command does not return the default values to the original default values.

The switch supports the following advertisement algorithm:

- Advertise all prefixes that are configured as addresses on the interface using the parameters defined by the `ipv6 nd prefix default` command (or the default value if the command has not been configured) except prefixes that are placed in the Prefix table (changed (configured) by the `ipv6 nd prefix` command).

- Advertise all prefixes configured by the `ipv6 nd prefix` command without the `no-advertise` keyword.

**Default Keyword**

The `default` keyword can be used to set default values for automatic advertised prefixes configured as addresses on the interface using the `ipv6 address` command.

**Note.** These default values are not used as the default values in the `ipv6 nd prefix` command.

Use the `no ipv6 nd prefix default` command to return the default values to the original default values.
On-Link

When on-link is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. An on-link prefix is inserted into the routing table as a Connected prefix.

Auto-configuration

When auto-configuration is on (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 auto-configuration.

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 ND Router Advertisement, and presence of the prefix in the routing table, as follows:

- **Default** L=1 A=1, In the Routing Table
- **no-onlink** L=0 A=1, In the Routing Table
- **no-autoconfig** L=1 A=0, In the Routing Table
- **no-onlink no-autoconfig** L=0 A=0, In the Routing Table
- **off-link** L=0 A=1, Not in the Routing Table
- **off-link no-autoconfig** L=0 A=0, Not in the Routing Table

Example

**Example 1.** The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out VLAN 1 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds. The prefix is inserted in the Routing table:

```
interface vlan 1
  ipv6 nd prefix 2001:0DB8::/35 1000 900
exit
```

**Example 2.** The following example advertises the prefix with the L-bit clear:

```
interface vlan 1
  ipv6 address 2001::/64
  ipv6 nd prefix 2001::/64 3600 3600 no-onlink
exit
```
**46.21 ipv6 nd ra interval**

Use the `ipv6 nd ra interval` command in Interface Configuration mode to configure the interval between IPv6 router advertisement (RA) transmissions on an interface. To restore the default interval, use the `no` form of this command.

**Syntax**

```
ipv6 nd ra interval maximum-secs [minimum-secs]
no ipv6 nd ra interval
```

**Parameters**

- `maximum-secs`—Maximum interval between IPv6 RA transmissions in seconds. The range is from 4 to 1800.
- `minimum-secs`—Minimum interval between IPv6 RA transmissions in seconds. The range is from 3 to 1350.

**Default Configuration**

- `maximum-secs` is 600 seconds.
- `minimum-secs` is `0.33 * maximum-secs`, if the value is $\geq$ 3 seconds and is 3 seconds, if the value is $< 3$ seconds.

**Command Mode**

Interface Configuration

**User Guidelines**

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.
Example

Example 1. The following example configures an IPv6 router advertisement interval of 201 seconds for VLAN 1:

```plaintext
interface vlan 1
  ipv6 nd ra interval 201
exit
```

Example 2. The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```plaintext
interface vlan 1
  ipv6 nd ra interval 200 50
exit
```

### 46.22 ipv6 nd ra lifetime

Use the `ipv6 nd ra lifetime` command in Interface Configuration mode to configure the Router Lifetime value in IPv6 router advertisements on an interface.

To restore the default lifetime, use the `no` form of this command.

**Syntax**

```
ipv6 nd ra lifetime seconds
no ipv6 nd ra lifetime
```

**Parameters**

`seconds`—Remaining length of time, in seconds, that this router will continue to be useful as a default router (Router Lifetime value). A value of zero indicates that it is no longer useful as a default router. The acceptable range is 0 or from `<Maximum RA Interval>` to 9000 seconds.

**Default Configuration**

The default lifetime value is `3*<Maximum RA Interval>` seconds.
**Command Mode**

Interface Configuration

**User Guidelines**

The Router Lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The Router Lifetime value can be set to a non-zero value to indicate that it should be considered a default router on this interface. The non-zero value for the Router Lifetime value should not be less than the router advertisement interval.

**Example**

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for VLAN 1:

```
interface vlan 1
  ipv6 nd ra lifetime 1801
exit
```

**46.23 ipv6 nd ra suppress**

Use the `ipv6 nd ra suppress` command in Interface Configuration mode to suppress IPv6 router advertisement transmissions on an interface. To re-enable the sending of IPv6 router advertisement transmissions on an interface, use the `no` form of this command.

**Syntax**

```
ipv6 nd ra suppress
no ipv6 nd ra suppress
```

**Parameters**

N/A.

**Default Configuration**

- **LAN interface** - IPv6 router advertisements are automatically sent.
- **Point-to-Point interface** - IPv6 router advertisements are suppressed.
NBMA interface - IPv6 router advertisements are suppressed.

**Command Mode**

Interface Configuration

**User Guidelines**

Use the `no ipv6 nd ra suppress` command to enable the sending of IPv6 router advertisement transmissions on a Point-to-Point interface (for example, manual tunnel).

Use the `no ipv6 nd ra suppress` command to enable the sending of IPv6 router advertisement transmissions on a NBMA interface (for example, ISATAP tunnel).

**Example**

**Example 1.** The following example suppresses IPv6 router advertisements on vlan 1:

```plaintext
interface vlan 1
    ipv6 nd ra suppress
exit
```

**Example 2.** The following example enables the sending of IPv6 router advertisements on tunnel 1:

```plaintext
interface tunnel 1
    no ipv6 nd ra suppress
exit
```

**46.24 ipv6 nd reachable-time**

Use the `ipv6 nd reachable-time` command in Interface Configuration mode to configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

To restore the default time, use the `no` form of this command.
Syntax

ipv6 nd reachable-time milliseconds

no ipv6 nd reachable-time

Parameters

milliseconds—Amount of time that a remote IPv6 node is considered reachable (in milliseconds). The acceptable range is from 0 to 3600000 milliseconds.

Default Configuration

0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration

User Guidelines

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.

Example

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for VLAN 1:

```
interface vlan 1
  ipv6 nd reachable-time 1700000
exit
```

46.25  ipv6 nd router-preference

Use the `ipv6 nd router-preference` command in Interface Configuration mode to configure a default router preference (DRP) for the router on a specific interface.
To return to the default DRP, use the `no` form of this command.

**Syntax**

```
ipv6 nd router-preference {high | medium | low}
```

```
no ipv6 nd router-preference
```

**Parameters**

- `high`—Preference for the router specified on an interface is high.
- `medium`—Preference for the router specified on an interface is medium.
- `low`—Preference for the router specified on an interface is low.

**Default Configuration**

Router advertisements (RAs) are sent with the medium preference.

**Command Mode**

Interface Configuration

**User Guidelines**

RA messages are sent with the DRP configured by this command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

**Example**

The following example configures a DRP of high for the router on VLAN 1:

```
interface vlan 1

    ipv6 nd router-preference high

exit
```
**46.26 ipv6 neighbor**

Use the `ipv6 neighbor` command in Global Configuration mode to configure a static entry in the IPv6 neighbor discovery cache. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the `no` form of this command.

**Syntax**

```
ipv6 neighbor ipv6-address interface-id mac-address
no ipv6 neighbor [ipv6-address] interface-id
```

**Parameters**

- `ipv6-address`—Specified IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `interface-id`—Specified interface identifier.

- `mac-address`—Interface MAC address.

**Default Configuration**

Static entries are not configured in the IPv6 neighbor discovery cache.

**Command Mode**

Global Configuration

**User Guidelines**

This command is similar to the `arp` (global) command.

Use the `ipv6 neighbor` command to add a static entry in the IPv6 neighbor discovery cache.

If the specified IPv6 address is a global IPv6 address it must belong to one of static on-link prefixes defined in the interface. When a static on-link prefix is deleted all static entries in the IPv6 neighbor discovery cache corresponding the prefix is deleted to.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache, learned through the IPv6 neighbor discovery process, the entry is automatically converted to a static entry.

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.
Use the `no ipv6 neighbor ipv6-address interface-id` command to remove the one given static entry on the given interface. The command does not remove the entry from the cache, if it is a dynamic entry, learned from the IPv6 neighbor discovery process.

Use the `no ipv6 neighbor interface-id` command to delete the all static entries on the given interface.

Use the `no ipv6 neighbor` command to remove the all static entries on all interfaces.

Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- NCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

**Note.** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries.

**Example**

**Example 1.** The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
ipv6 neighbor 2001:0DB8::45A vlan1 0002.7D1A.9472
```

**Example 2.** The following example deletes the static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
no ipv6 neighbor 2001:0DB8::45A vlan1
```

**Example 3.** The following example deletes all static entries in the IPv6 neighbor discovery cache on VLAN 1:

```
no ipv6 neighbor vlan1
```
Example 4. The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
no ipv6 neighbor
```

### 46.27 ipv6 prefix-list

Use the `ipv6 prefix-list` command in Global Configuration mode to create an entry in an IPv6 prefix list. To delete the entry, use the `no` form of this command.

**Syntax**

```
ipv6 prefix-list list-name [seq number] {{deny|permit} ipv6-prefix/prefix-length [ge ge-length] [le le-length] | description text

no ipv6 prefix-list list-name [seq number]
```

**Parameters**

- **list-name**—Name of the prefix list. The name may contain up to 32 characters.
- **seq seq-number**—Sequence number of the prefix list entry being configured. This is an integer value from 1 to 4294967294.
- **deny**—Denies networks that matches the condition.
- **permit**—Permits networks that matches the condition.
- **ipv6-prefix**—IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
- **/prefix-length**—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value from 0 to 128. The zero prefix-length may be used only with the zero ipv6-prefix (::).
- **description text**—Text that can be up to 80 characters in length.
- **ge ge-value**—Specifies a prefix length greater than or equal to the `ipv6-prefix/prefix-length` arguments. It is the lowest value of a range of the length (the “from” portion of the length range).
- **le le-value**—Specifies a prefix length less than or equal to the `ipv6-prefix/prefix-length` arguments. It is the highest value of a range of the length (the “to” portion of the length range).

**Default Configuration**

No prefix list is created.

**Command Mode**

Global Configuration

**User Guidelines**

This command without the **seq** keyword adds the new entry after the last entry of the prefix list with the sequence number equals to the last number plus 5. For example, if the last configured sequence number is 43, the new entry will have the sequence number of 48. If the list is empty, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.

This command with the **seq** keyword puts the new entry into the place specified by the parameter, if an entry with the number exists it is replaced by the new one.

This command without the **seq** keyword removes the prefix list.

The no version of this command with the **seq** keyword removes the specified entry.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you might want to put the most common permits or denies near the top of the list, using the seq-number argument.

The `show ipv6 prefix-list` command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual `ipv6-prefix/prefix-length` argument.
For a candidate prefix to match against a prefix list entry the following conditions must exist:

- The candidate prefix must match the specified prefix list and prefix length entry
- The value of the optional le keyword specifies the range of allowed prefix lengths from the prefix-length argument up to, and including, the value of the le keyword
- The value of the optional ge keyword specifies the range of allowed prefix lengths from the value of the ge keyword up to, and including, 128.

Note that the first condition must match before the other conditions take effect.

An exact match is assumed when the ge or le keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The prefix-length value must be less than the ge value. The ge value must be less than, or equal to, the le value. The le value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have permit and deny condition statements, has an implicit deny any any statement as its last match condition.

**Formal Specification**

Checked prefix is cP and checked prefix length is cL.

Function PrefixIsEqual(P1, P2, L) compares the first L bits of two addresses P1 and P2 and returns TRUE if they are equal.

Case 1. A prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is not defined
- le - is not defined

The prefix cP/cL matches the prefix-list entry if PrefixIsEqual(cP,P1) && cL == L

Case 2. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is defined

The value of the optional ge keyword specifies the range of allowed prefix lengths from the value of the ge keyword up to, and including, 128.
The prefix cP/cL matches the prefix-list entry if $$\text{PrefixIsEqual}(cP, P, L) \&\& cL \geq ge$$

**Case 3.** An prefix-list entry is:
- \(P\) - prefix address
- \(L\) - prefix length
- \(ge\) - is not defined
- \(le\) - is defined

The prefix cP/cL matches to the prefix-list entry if $$\text{PrefixIsEqual}(cP, P, L) \&\& cL \leq le$$

**Case 4.** An prefix-list entry is:
- \(P\) - prefix address
- \(L\) - prefix length
- \(ge\) - is defined
- \(le\) - is defined

The prefix cP/cL matches the prefix-list entry if $$\text{PrefixIsEqual}(cP, P, L) \&\& ge \leq cL \leq le$$

**Example**

**Example 1.** The following example denies all routes with a prefix of ::/0:

```
switchxxxx(config)#ipv6 prefix-list abc deny ::/0
```

**Example 2.** The following example permits the prefix 2002::/16:

```
switchxxxx(config)#ipv6 prefix-list abc permit 2002::/16
```

**Example 3.** The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64:

```
switchxxxx(config)#ipv6 prefix-list abc permit 5F00::/48 le 64
```
Example 4. The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64:

```
switchxxxx(config)ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

Example 5. The following example permits mask lengths from 32 to 64 bits in all address space:

```
switchxxxx(config)ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

Example 6. The following example denies mask lengths greater than 32 bits in all address space:

```
switchxxxx(config)ipv6 prefix-list abc deny ::/0 ge 32
```

Example 7. The following example denies all routes with a prefix of 2002::/128:

```
switchxxxx(config)ipv6 prefix-list abc deny 2002::/128
```

Example 8. The following example permits all routes with a prefix of ::/0:

```
switchxxxx(config)ipv6 prefix-list abc permit ::/0
```

### 46.28 ipv6 redirect

Use the `ipv6 redirects` command in Interface Configuration mode to enable the sending of ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received.

To disable the sending of redirect messages, use the `no` form of this command.

**Syntax**

ipv6 redirect

no ipv6 redirect
Parameters
N/A.

Default Configuration
The sending of ICMP IPv6 redirect messages is enabled.

Command Mode
Interface Configuration.

User Guidelines
The rate at which the router generates all IPv6 ICMP error messages can be limited by using this command.

Example
The following example disables the sending of ICMP IPv6 redirect messages on VLAN 100 and re-enables the messages on VLAN 2:

```plaintext
interface vlan 100
  no ipv6 redirect
exit
interface vlan 2
  ipv6 redirect
exit
```

46.29 ipv6 route
Use the ipv6 route command in Global Configuration mode to establish static IPv6 routes.
To remove a previously configured static route, use the no form of this command.

Syntax
ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id} [metric]
no ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id}
Parameters

- **ipv6-prefix**—IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.

- **/prefix-length**—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

- **next-ipv6-address**—IPv6 address of the next hop that can be used to reach the specified network.
  - If the `next-ipv6-address` argument is a link local address it must be defined in the zone format: IPv6 Zone Format> ::= IPv6-Link-Local-Address%Interface-ID
  - The `interface-id` argument must be coded without spaces.

- **interface-id**—Outgoing Interface identifier.

- **metric**—Static route metric. Acceptable values are from 1 to 65535. The default value is 1.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration

User Guidelines

If the next IPv6 address is a global IPv6 address, it should belong to a static on-link prefix. When an on-link prefix is removed or is changed to non on-link prefix, the static routes with next hop belonging to the prefix are removed from the configuration.

The `interface-id` argument can be defined only on a point-to-point interface.

Example

**Example 1.** The following example defines a static route with a global next hop:

```
ipv6 route 2001::/64 5::5
```
Example 2. The following example defines a static route on point-to-point tunnel 1:

```
ipv6 route 2001:DB8:2222::/48 tunnel1
```

Example 3. The following example defines a static route with a link-local next hop:

```
ipv6 route 2001:DB8:2222::/48 FE80::260:3EFF:FE11:6770%vlan1
```

### 46.30 ipv6 unicast-routing

Use the `ipv6 unicast-routing` command in Global Configuration mode to enable the forwarding of IPv6 Unicast datagrams.

To disable the forwarding of IPv6 Unicast datagrams, use the `no` form of this command.

**Syntax**

- `ipv6 unicast-routing`
- `no ipv6 unicast-routing`

**Parameters**

- N/A.

**Default Configuration**

IPv6 Unicast routing is disabled.

**Command Mode**

Global Configuration

**Example**

The following example enables the forwarding of IPv6 Unicast datagrams:

```
ipv6 unicast-routing
```
46.31 ipv6 unreachables

Use the `ipv6 unreachables` command in Interface Configuration mode to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.

To prevent the generation of unreachable messages, use the `no` form of this command.

Syntax

```
ipv6 unreachables
no ipv6 unreachables
```

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode

Interface Configuration.

User Guidelines

If the switch receives a Unicast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the switch receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Example

The following example disables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
interface vlan 100
  no ipv6 unreachables
exit
```
### 46.32 **show ipv6 interface**

Use the **show ipv6 interface** command in user EXEC or privileged EXEC mode to display the usability status of interfaces configured for IPv6.

**Syntax**

```
show ipv6 interface [brief] | [[interface-id] [prefix]]
```

**Parameters**

- **brief**—Displays a brief summary of IPv6 status and configuration for each interface where IPv6 is defined.
- **interface-id**—Interface identifier about which to display information.
- **prefix**—Prefix generated from a local IPv6 prefix pool.

**Default Configuration**

Option **brief** - all IPv6 interfaces are displayed.

**Command Mode**

- User EXEC
- Privileged EXEC

**User Guidelines**

Use this command to validate the IPv6 status of an interface and its configured addresses. This command also displays the parameters that IPv6 uses for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up.

If you specify an optional interface identifier, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

**Example**

**Example 1.** The **show ipv6 interface** command displays information about the specified interface:

```
show ipv6 interface vlan 1
```
VLAN 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):

<table>
<thead>
<tr>
<th>IPv6 Global Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:0DB8::2/64 (ANY)</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:0DB8::2/64</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:1DB8::2011/64</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Joined group address(es):
- FF02::1
- FF02::2
- FF02::1:FF11:6770

MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router maximum advertisement interval is 600 seconds
ND router minimum advertisement interval is 198 seconds (DEFAULT)
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Stateless autoconfiguration is enabled
MLD Version is 2

Field Descriptions:

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked Enabled. If duplicate address detection processing identified the link-local address of the
interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked Stalled. If IPv6 is not enabled, the interface is marked Disabled.

- **link-local address**—Displays the link-local address assigned to the interface.
- **Global unicast address(es)**—Displays the global Unicast addresses assigned to the interface. The type is manual or autoconfig.
- **Joined group address(es)**—Indicates the Multicast groups to which this interface belongs.
- —Maximum transmission unit of the interface.
- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- **ICMP redirects**—State of ICMP IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).
- **number of DAD attempts**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.
- **ND advertised default router preference is Medium**—DRP for the router on a specific interface.
- **MLD Version**—Version of MLD
Example 2. The `show ipv6 interface` command displays information about the specified manual IPv6 tunnel:

```
show ipv6 interface tunnel 2

Tunnel 2 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):

<table>
<thead>
<tr>
<th>Ipv6 Global Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:0DB8::2/64 (ANY)</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:0DB8::2/64</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:1DB8::2011/64</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Joined group address(es):

FF02::1
FF02::2
FF02::1:FF11:6770

MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
MLD Version is 2
Tunnel mode is manual
Tunnel Local IPv4 address : 10.10.10.1(auto)
Tunnel Remote Ipv4 address : 10.1.1.1
```
Field Descriptions:

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.

- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”

- **link-local address**—Displays the link-local address assigned to the interface.

- **Global Unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is manual or autoconfig.

- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.

- **—Maximum transmission unit of the interface.**

- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.

- **ICMP redirects**—The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).

- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).

- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.

- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.

- **ND advertised default router preference is Medium**—The DRP for the router on a specific interface.

- **MLD Version**—The version of MLD

- **Tunnel mode**—Specifies the tunnel mode: `manual`, `6to4`, `auto-tunnel` or `isatap`

- **Tunnel Local IPv4 address**—Specifies the tunnel local IPv4 address and have one of the following formats:
  - `ipv4-address`
  - `ipv4-address (auto)`
  - `ipv4-address (interface-id)`

- **Tunnel Remote IPv4 address**—Specifies the tunnel remote IPv4 address

---

**Example 3.** The `show ipv6 interface` command displays information about the specified ISATAP tunnel:

```
show ipv6 interface tunnel 1

Tunnel 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
ICMP redirects are disabled
Global unicast address(es):
  Ipv6 Global Address                         Type
  2000:0DB8::2/64 (ANY)                       Manual
  2000:0DB8::2/64                              Manual
  2000:1DB8::2011/64                          Manual
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF11:6770
```
is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is disabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
MLD Version is 2
Tunnel mode is ISATAP
Tunnel Local IPv4 address : 10.10.10.1(VLAN 1)
ISATAP Router DNS name is isatap

Field Descriptions:

- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled). Note. The state of duplicate address detection on an IPv6 tunnel interface of ISATAP type always is displayed as disabled regardless of a value of the number of DAD attempts parameter because DAD is not supported on NBMA interfaces. The switch will enable DAD automatically when the user change the type of the tunnel to manual if a the parameter value bigger than 0.

- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.

- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”
- **link-local address**—Displays the link-local address assigned to the interface.

- **Global Unicast address(es)**—Displays the global Unicast addresses assigned to the interface. The type is `manual` or `autoconfig`.

- **Joined group address(es)**—Indicates the Multicast groups to which this interface belongs.

- **Maximum transmission unit of the interface.**

- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.

- **ICMP redirects**—The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).

- **number of DAD attempts**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.

- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.

- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.

- **ND advertised default router preference is Medium**—The DRP for the router on a specific interface.

- **MLD Version**—The version of MLD

- **Tunnel mode**—Specifies the tunnel mode: `manual`, `6to4`, `auto-tunnel` or `isatap`

- **Tunnel Local IPv4 address**—Specifies the tunnel local IPv4 address and have one of the following formats:
  - `ipv4-address`
  - `ipv4-address (auto)`
- `ipv4-address (interface-id)`
  - **Tunnel Remote IPv4 address**—Specifies the tunnel remote IPv4 address
  - **ISATAP Router DNS name is**—The DNS name of the ISATAP Router

**Example 4.** The following command with the *brief* keyword displays information about all interfaces that IPv6 is defined on:

```plaintext
Router# show ipv6 interface brief
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface IPv6 State</th>
<th>Link Local IPv6 Address</th>
<th>MLD Version</th>
<th>Number of Global Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa1/0/10</td>
<td>up/up enabled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>fa1/0/11</td>
<td>up/up stalled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>fa1/0/12</td>
<td>up/down enabled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>po1</td>
<td>down/down enabled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>tunnel 1</td>
<td>up/up enabled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vlan 1</td>
<td>up/up enabled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vlan 1000</td>
<td>up/up stalled</td>
<td>FE80::0DB8:12AB:FA01</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Example 5.** This sample output shows the characteristics of VLAN 1 that has generated a prefix from a local IPv6 prefix pool:

```plaintext
interface vlan1
  ipv6 address 2001:0DB8:1::1/64
  ipv6 address 2001:0DB8:2::1/64
  ipv6 address 2001:0DB8:3::1/64
  ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
  ipv6 nd prefix 2001:0DB8:3::/64 2912000 564900 off-link
  ipv6 nd prefix 2001:0DB8:4::/64
  ipv6 nd prefix 2001:0DB8:5::/64 2912000 564900 off-link
exit
```
show ipv6 interface vlan 1 prefix
IPv6 Prefix Advertisements VLAN 1
Codes: A - Address, P - Prefix is advertised, R is in Routing Table
<table>
<thead>
<tr>
<th>Code</th>
<th>Prefix</th>
<th>Flags</th>
<th>Valid Lifetime</th>
<th>Preferred Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>--------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>default</td>
<td></td>
<td>LA</td>
<td>2592000</td>
<td>604800</td>
</tr>
<tr>
<td>AR</td>
<td>2001:0DB8:1::/64</td>
<td>LA</td>
<td>infinite</td>
<td>infinite</td>
</tr>
<tr>
<td>APR</td>
<td>2001:0DB8:2::/64</td>
<td>LA</td>
<td>infinite</td>
<td>infinite</td>
</tr>
<tr>
<td>AP</td>
<td>2001:0DB8:3::/64</td>
<td>A</td>
<td>infinite</td>
<td>infinite</td>
</tr>
<tr>
<td>PR</td>
<td>2001:0DB8:4::/64</td>
<td>LA</td>
<td>2592000</td>
<td>604800</td>
</tr>
<tr>
<td>P</td>
<td>2001:0DB8:5::/64</td>
<td>A</td>
<td>2912000</td>
<td>564900</td>
</tr>
</tbody>
</table>

**46.33 show ipv6 link-local default zone**

Use the `show ipv6 link-local default zone` command in user EXEC or privileged EXEC mode to display the IPv6 link local default zone.

**Syntax**

`show ipv6 link-local default zone`

**Command Mode**

EXEC mode

Privileged EXEC

**Example**

**Example 1.** The following example displays the default zone when it is defined:

`show ipv6 link-local default zone`

Link Local Default Zone is VLAN 1
Example 2. The following example displays the default zone when it is not defined:

```
show ipv6 link-local default zone
Link Local Default Zone is not defined
```

46.34 show ipv6 nd prefix

Use the `show ipv6 nd prefix` command in user EXEC or privileged EXEC mode to display IPv6 prefixes included in IPv6 Neighbor Discovery (ND) router advertisements.

**Syntax**

```
show ipv6 nd prefix [interface-id]
```

**Parameters**

- **interface-id**—Specified interface identifier on which prefixes are advertised.

**Default Configuration**

No prefixes are displayed.

**Command Mode**

EXEC mode

Privileged EXEC

**User Guidelines**

Use the `show ipv6 nd prefix` command with the `interface-id` argument to display prefixes advertised on a single interface.

**Example**

The following example displays IPv6 prefixes:

```
show ipv6 nd prefix vlan 100
vlan 100
  default
    valid-lifetime 2,592,000 secs
```
preferred-lifetime 604,800 secs
on-link
auto-config
prefix 2001::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
prefix 2001:2:12/64
  no advertise
prefix 2002::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
on-link
prefix 2011::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
off-link
auto-config

46.35  show ipv6 neighbors

Use the show ipv6 neighbors command in User EXEC or Privileged EXEC mode to display IPv6 neighbor discovery (ND) cache information.

Syntax

show ipv6 neighbors [interface-id\ ipv6-address\ ipv6-hostname]

Parameters

- interface-id—Specifies the identifier of the interface from which IPv6 neighbor information is to be displayed.
- ipv6-address—Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
• **ipv6-hostname**—Specifies the IPv6 host name of the remote networking device.

**Default Configuration**

All IPv6 ND cache entries are listed.

**Command Mode**

User EXEC

Privileged EXEC

**User Guidelines**

When the *interface-id* argument is not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-id* argument displays only cache information about the specified interface.

**Example**

**Example 1.** The following is sample output from the show ipv6 neighbors command when entered with an *interface-id*:

```
show ipv6 neighbors  vlan  1
IPv6 Address    Age  Link-layer Addr  State  Interface  Router
2000:0:0:4::2    0     0003.a0d6.141e  REACH VLAN1 Yes
3001:1::45a     -     0002.7d1a.9472  REACH VLAN1 -
FE80::203:AFF:FE66:141E  0     0003.a0d6.141e  REACH VLAN1 No
```

**Example 2.** The following is sample output from the show ipv6 neighbors command when entered with an IPv6 address:

```
show ipv6 neighbors 2000:0:0:4::2
IPv6 Address    Age  Link-layer Addr  State  Interface  Router
2000:0:0:4::2    0     0003.a0d6.141e  REACH VLAN1 Yes
```

**Field Descriptions:**

- **Total number of entries**—Number of entries (peers) in the cache.
- **IPv6 Address**—IPv6 address of neighbor or interface.
- **Age**—Time (in minutes) since the address was confirmed to be reachable. A hyphen (−) indicates a static entry.
- **Link-layer Addr**—MAC address. If the address is unknown, a hyphen (−) is displayed.
- **Interface**—Interface which the neighbor is connected to.
- **Router**—Specifies if the neighbor is a Router. A hyphen (−) is displayed for static entries.

### 46.36  show ipv6 prefix-list

Use the `show ipv6 prefix-list` command in user EXEC or privileged EXEC mode to display information about an IPv6 prefix list or IPv6 prefix list entries.

**Syntax**

```
show ipv6 prefix-list [detail [list-name] | summary [list-name]]
show ipv6 prefix-list list-name ipv6-prefix/prefix-length [longer | first-match]
show ipv6 prefix-list list-name seq seq-num
```

**Parameters**

- **detail | summary**—Displays detailed or summarized information about all IPv6 prefix lists.
- **list-name**—Name of a specific IPv6 prefix list.
- **ipv6-prefix**—All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- **longer**—Displays all entries of an IPv6 prefix list that are more specific than the given ipv6-prefix/prefix-length values.
- **first-match**—Displays the entry of an IPv6 prefix list that matches the given ipv6-prefix/prefix-length values.
- **seq seq-num**—Sequence number of the IPv6 prefix list entry.
Command Mode

User EXEC
Privileged EXEC

User Guidelines

If the **detail** and **summary** keywords are omitted, the **detail** option is applied.

If the **longer** and **first-match** keywords are omitted, all entries of the specified prefix list that matches the given network/length are displayed.

Example

**Example 1.** The following example shows the output of this command with the **detail** keyword:

```
switchxxxxxx#show ipv6 prefix-list detail
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
  seq 5 permit 2002::/16 (hit count: 313)
ipv6 prefix-list aggregate:
  count: 3, range entries: 2
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568)
  seq 10 description The Default Action
  seq 15 permit ::/0 le 48 (hit count: 31310)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3
  seq 5 deny 5F00::/8 le 128 (hit count: 0)
  seq 10 deny ::/0 (hit count: 0)
  seq 15 deny ::/1 (hit count: 0)
  seq 20 deny ::/2 (hit count: 0)
  seq 25 deny ::/3 ge 4 (hit count: 0)
  seq 30 permit ::/0 le 128 (hit count: 240664)
```

Field Descriptions
• **count**—Number of entries in the list.
• **range entries**—Number of entries with matching range.
• **seq**—Entry number in the list.
• **permit, deny**—Granting status.
• **description**—Comment.
• **hit count**—Number of matches for the prefix entry.

**Example 2.** The following example shows the output of the `show ipv6 prefix-list` command with the `summary` keyword:

```
switchxxxxxx#show ipv6 prefix-list summary
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
ipv6 prefix-list aggregate:
  count: 2, range entries: 2
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3
```

**Example 3.** The following example shows the output of the `show ipv6 prefix-list` command with the `seq` keyword:

```
switchxxxxxx#show ipv6 prefix-list bgp-in seq 15
  seq 15 deny ::/1 (hit count: 0)
```

### 46.37 show ipv6 route

Use the `show ipv6 route` command in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.

**Syntax**

```
show ipv6 route [ipv6-address|ipv6-prefix/prefix-length|protocol|interface interface-id]
```
Parameters

- `ipv6-address`—Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `ipv6-prefix`—Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `/prefix-length`—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

- `protocol`—Displays routes for the specified type of route using any of these keywords: connected, static, nd, or icmp.

- `interface interface-id`—Identifier of an interface.

Default Configuration

All IPv6 routing information for all active routing tables is displayed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

This command provides output similar to the `show ip route` command, except that the information is IPv6-specific.

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When the icmp, nd, connected, local, or static keywords are specified, only that type of route is displayed. When the `interface-id` argument are specified, only the specified interface-specific routes are displayed.
Example

Example 1. The following is sample output from the `show ipv6 route` command when IPv6 Routing is not enabled and the command is entered without an IPv6 address or prefix specified:

```
switchxxxxxx#show ipv6 route
Codes: > - Best
        S - Static, I - ICMP Redirect, ND - Router Advertisement
        [d/m]: d - route’s distance, m - route’s metric
IPv6 Routing Table - 6 entries
S> ::/0 [1/1]
    via fe80::77 VLAN 1
ND> ::/0 [11/0]
    via fe80::200:cf:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
ND> 2001::/64 [0/0]
    via :: VLAN 100
ND> 2002:1:1::/64 [0/0]
    via :: VLAN 100
ND> 3001::/64 [0/0]
    via :: VLAN 101
ND> 4004::/64 [0/0]
    via :: VLAN 110
```

Example 2. The following is sample output from the `show ipv6 route` command when IPv6 Routing is supported and the command is entered without an IPv6 address or prefix specified and IPv6 Routing is enabled:

```
switchxxxxxx#show ipv6 route
Codes: > - Best
        S - Static, C - Connected,
        L - Local(on-link prefixes defined by the `ipv6 nd prefix` command with `on-link` keyword,
```
O - OSPF intra-area, OIA - OSPF inter-area,
OE1 - OSPF external 1, OE2 - OSPF external 2,
B - BGP

[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 5 entries
IPv6 Routing Table - 5 entries
IPv6 Routing Table - 3 entries

S>  3000::/64 [1/1]
   via FE80::A8BB:CCFF:FE02:8B00   VLAN 100

OE1> 4000::/128 [0/0]
   via FE80::A8BB:CCFF:FE02:8B01   VLAN 101

O>  4000::/64 [0/0]
   via FE80::A8BB:CCFF:FE02:8B02   VLAN 101

C>  4001::/64 [0/0]
   via ::   VLAN 100

L>  4002::/64 [0/0]
   via ::   VLAN 100 Lifetime 9000 sec

Example 3. The following is sample output from the show ipv6 route command when entered with the IPv6 prefix 2001:200::/35 and IPv6 Routing is supported:

```
switchxxxxxxx#show ipv6 route 2001:200::/35
Codes: > - Best
        S - Static, C - Connected,
        L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link keyword,
        O - OSPF intra-area, OIA - OSPF inter-area,
        OE1 - OSPF external 1, OE2 - OSPF external 2,
        B - BGP
```
Example 4. The following is sample output from the show ipv6 route command when IPv6 Routing is supported and the command is entered with the bgp keyword:

```
switchxxxxxx#show ipv6 route bgp

Codes: > - Best
       S - Static, C - Connected,
       L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link keyword,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP
[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 129 entries
O>  3000::/64 [20/0]
    via FE80::A8BB:CCFF:FE02:8B00 Tunnel1
```

46.38  show ipv6 route summary

Use the `show ipv6 route summary` command in User EXEC or Privileged EXEC mode to display the current contents of the IPv6 routing table in summary format.

Syntax

```
show ipv6 route summary
```
46.39 show ipv6 static

Use the `show ipv6 static` command in user EXEC or privileged EXEC mode to display the current static routes of the IPv6 routing table.

**Syntax**

```
show ipv6 static [ipv6-address | ipv6-prefix/prefix-length] [interface interface-id][detail]
```

**Parameters**

- `ipv6-address`—Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `ipv6-prefix`—Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- `/prefix-length`—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the...
prefix (the network portion of the address). A slash mark must precede the decimal value.

- `interface interface-id`—Identifier of an interface.
- `detail`—Specifies for invalid routes, the reason why the route is not valid.

Default Configuration
All IPv6 static routing information for all active routing tables is displayed.

Command Mode
User EXEC
Privileged EXEC

User Guidelines
When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the `interface-id` argument is specified, only the specified interface-specific routes are displayed.

When the `detail` keyword is specified, the reason why the route is not valid is displayed for invalid direct or fully specified routes.

Example

**Example 1.** The following is sample output from the `show ipv6 static` command without specified options:

```
switchxxxxxx#show ipv6 static
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
  5555::/16, via nexthop 4001:AF00::1, metric 1
```
Example 2. The following is sample output from the `show ipv6 route` command when entered with the IPv6 prefix 2001:200::/35:

```
switchxxxxxx# show ipv6 static 2001:200::/35
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
  * 2001:200::/35, via nexthop 4000::1, metric 1
  2001:200::/35, via nexthop 9999::1, metric 1
  * 2001:200::/35, interface VLAN1, metric 1
```

Example 3. The following is sample output from the `show ipv6 route` command when entered with the interface VLAN 1:

```
switchxxxxxx# show ipv6 static interface vlan 1
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
  * 5000::/16, interface VLAN1, metric 1
```

Example 4. The following is sample output from the `show ipv6 route` command with the `detail` keyword:

```
switchxxxxxx# show ipv6 static detail
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
  * 3000::/16, interface VLAN1, metric 1
  * 4000::/16, via nexthop 2001:1::1, metric 1
    5000::/16, interface fa 1/0/10, metric 1
    Interface is down
  * 5555::/16, via nexthop 4000::1, metric 1
    5555::/16, via nexthop 9999::1, metric 1
```
Route does not fully resolve

* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
## Tunnel Commands

### 47.1 interface tunnel

Use the `interface tunnel` Global Configuration mode command to enter the Interface Configuration (Tunnel) mode.

**Syntax**

`interface tunnel number`

**Parameters**

- `number`— Specifies the tunnel number.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**Example**

The following example enters the Interface Configuration (Tunnel) mode.

```
interface tunnel 1
  tunnel source auto
exit
```

### 47.2 tunnel destination

Use the `tunnel destination` command in Tunnel Interface Configuration mode to specify the destination for the manual tunnel interface. To remove the destination, use the `no` form of this command.

**Syntax**

`tunnel destination {host-name|ip-address}`
no tunnel destination

Parameters

- host-name — DNS name of the remote host.
- ip-address — IPv4 address of the remote host.

Default Configuration

No tunnel interface destination is specified.

Command Mode

Tunnel Interface Configuration

User Guidelines

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address.

Example

The following example shows how to configure the tunnel destination address for Manual IPv6 tunnel:

```
interface vlan 1
  ip address 10.0.0.1 255.255.255.0
exit
interface tunnel1
  ipv6 address 3ffe:b00:c18:1::3/127
  tunnel source vlan1
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
exit
```

47.3 tunnel isatap solicitation-interval

Use the `tunnel isatap solicitation-interval` Global Configuration mode command to set the time interval between unsolicited router solicitation messages. Use the `no` form of this command to restore the default configuration.
Syntax

tunnel isatap solicitation-interval seconds

no tunnel isatap solicitation-interval

Parameters

seconds—Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600)

Default Configuration

The default time interval between ISATAP router solicitation messages is 10 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command determines the interval between unsolicited router solicitation messages sent to discovery an ISATAP router.

Example

The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

---
tunnel isatap solicitation-interval 30
---

47.4 tunnel isatap robustness

Use the tunnel isatap robustness Global Configuration mode command to configure the number of router solicitation refresh messages that the device sends. Use the no form of this command to restore the default configuration.

Syntax

tunnel isatap robustness number

no tunnel isatap robustness
Tunnel Commands

Parameters

**number**— Specifies the number router solicitation refresh messages that the device sends. (Range: 1–20)

Default Configuration

The default number of router solicitation refresh messages that the device sends is 3.

Command Mode

Global Configuration mode

User Guidelines

The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

Example

The following example sets the number of router solicitation refresh messages that the device sends to 5.

```
tunnel isatap robustness 5
```

47.5  **tunnel isatap router**

Use the `tunnel isatap router` Interface Configuration (Tunneled) mode command to configure a global string that represents a specific automatic tunnel router domain name. Use the `no` form of this command to remove this router name and restore the default configuration.

Syntax

```
tunnel isatap router router-name

no tunnel isatap router
```

Parameters

**router-name**— Specifies the router’s domain name.
Default Configuration
The automatic tunnel router's default domain name is ISATAP.

Command Mode
Interface Configuration (Tunnel) mode

User Guidelines
This command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string ISATAP is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

The empty string means that automatic lookup is not applied.

Example
The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
interface tunnel 1
  tunnel isatap router ISATAP2
exit
```

47.6 tunnel mode ipv6ip
Use the `tunnel mode ipv6ip` command in Interface Configuration mode to configure a static IPv6 tunnel interface. To remove an IPv6 tunnel interface, use the `no` form of this command.

Syntax
```
tunnel mode ipv6ip [isatap]
```

Parameters
- **isatap**—Specifies IPv6 automatic tunneling mode as ISATAP to connect IPv6 nodes (hosts and routers) within IPv4 networks.
**Default Configuration**
IPv6 tunnel interfaces are not configured.

**Command Mode**
Tunnel Interface Configuration

**User Guidelines**
IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

The IPv6 interface is automatically enabled on a tunnel when it is configured as an IPv6 tunnel by the `tunnel mode ipv6ip` command and the local IPv4 is defined by the `tunnel source` command.

When the IPv6 tunnel mode is changed the IPv6 interface on the tunnel is re-enabled that causes removing static IPv6 configuration on the tunnel (for example, global IPv6 addresses, static IPv6 routes via the tunnel, etc.).

The IPv6 interface on an IPv6 tunnel is disabled if the tunnel stops to be an IPv6 tunnel or the tunnel local IPv4 address is removed and the new IPv4 cannot be chosen.

**Manually Configured Tunnels**
Using this command without keywords specifies an IPv6-configured tunnel where the tunnel endpoints is determined by two manually configured unique IPv4 addresses by the `tunnel source` and `tunnel destination` commands. Only the `ipv6 address eui-64` command can be used to configured a global unicast IPv6 on a manual tunnel. Any correct global 64-bits IPv6 prefix can be configured.

The interface identifier of tunnel is 0:0:WWXX:YYZZ, where WWXX:YYZZ is the tunnel local IPv4 address (RFC 4213).

Only the `ipv6 address eui-64` command can be used to configured a global unicast IPv6 on a manual tunnel. Any correct global 64-bits IPv6 prefix can be configured.

The interface identifier of tunnel is 0:0:WWXX:YYZZ, where WWXX:YYZZ is the tunnel local IPv4 address (RFC 4213).

**ISATAP Tunnels**
Using this command with the `isatap` keyword specifies an automatic ISATAP tunnel. ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.
ISATAP IPv6 addresses can use any initial Unicast /64 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address. Only the *ipv6 address eui-64* command can be used to configure a global unicast IPv6 on a manual tunnel.

**Example**

**Example 1**— The following example configures an ISATAP tunnel:

```plaintext
interface vlan 1
  ip address 1.1.1.1 255.255.255.0
exit
interface tunnel 1
  tunnel mode ipv6ip isatap
  tunnel source 1.1.1.1
  ipv6 address 3ffe:b00:c18:1::/64 eui-64
exit
```

**Example 2**— The following example configures a manual IPv6 tunnel. In the example, tunnel interface 1 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured:

```plaintext
interface tunnel 1
  tunnel source vlan 1
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
exit
```

### 47.7 tunnel source

Use the *tunnel source* Interface Configuration (Tunnel) mode command to set the local (source) IPv4 address of a tunnel interface. The *no* form deletes the tunnel local address.
**Syntax**

*tunnel source {auto | ipv4-address | interface-id}*

*no tunnel source*

**Parameters**

- **auto**—The system minimum IPv4 address is used as the local IPv4 address (IPv4 address of the local tunnel endpoint).
- **ipv4-address**—Specifies the IPv4 address to use as the local IPv4 address (IPv4 address of the local tunnel endpoint).
- **interface-id**—Interface which the minimum IPv4 address is used as the local IPv4 address (IPv4 address of the local tunnel endpoint).

**Default**

No source address is defined.

**Command Mode**

Interface Configuration (Tunnel) mode

**User Guidelines**

If the **auto** or **interface-id** option is configured once time chosen IPv4 is used as the tunnel local IPv4 address until it is defined. A new IPv4 interface is only chosen in the following cases:

- After reboot.
- The used IPv4 is removed from the switch configuration.
- The tunnel mode is changed.

When the tunnel local IPv4 address is changed the IPv6 interface on the tunnel is re-enabled that causes removing static IPv6 configuration on the tunnel (for example, global IPv6 addresses, static IPv6 routes via the tunnel, etc.).

**Example**

```plaintext
interface tunnel 1
  tunnel source 120.12.3.4
exit
```
47.8  show ipv6 tunnel

Use the `show ipv6 tunnel` EXEC mode command to display information on the ISATAP tunnel.

Syntax

`show ipv6 tunnel [all]`

Parameters

- **all**—The switch displays all parameters of the tunnel. If the keyword is not configured only the tunnel parameters corresponding to its type are displayed.

Command Mode

EXEC mode

Example

**Example 1.** The following example displays information on the ISATAP tunnel, when the all keyword is not configured:

```
switchxxxxxx#  show ipv6 tunnel
Tunnel 1
  Tunnel type : Manual
  Tunnel status : UP
  Tunnel Local address type : VLAN 100
  Tunnel Local Ipv4 address : 192.1.3.4
  Tunnel Remote Ipv4 address : 192.3.4.5
Tunnel 2
  Tunnel type : ISATAP
  Tunnel status : UP
  Tunnel Local address type : auto
  Tunnel Local Ipv4 address : 192.1.3.4
  Router DNS name : ISATAP
  Router IPv4 addresses
    1.1.1.1          Detected
```
Example 2. The following example displays information when the all keyword is configured:

```
switchxxxxxx# show ipv6 tunnel all

Tunnel 1
Tunnel type : Manual
Tunnel status : UP
Tunnel Local address type : VLAN 100
Tunnel Local Ipv4 address : 192.1.3.4
Manual parameters
  Tunnel Remote Ipv4 address : 192.3.4.5
ISATAP Parameters
  Router DNS name : ISATAP
  Router Solicitation interval : 10 seconds
  Robustness : 2

Tunnel 2
Tunnel type : ISATAP
Tunnel status : UP
Tunnel Local address type : auto
Manual parameters
  Tunnel Remote Ipv4 address : 0.0.0.0
ISATAP Parameters
  Tunnel Local Ipv4 address : 192.1.3.4
  Router DNS name : ISATAP
```
Tunnel Commands

Router IPv4 addresses
1.1.1.1          Detected
100.1.1.1        Detected
14.1.100.1       Not Detected

Router Solicitation interval : 10 seconds

Robustness : 2

Tunnel 3
Tunnel type : Manual
Tunnel status : DOWN
Tunnel Local address type : auto

Manual parameters
Tunnel Remote IPv4 address : 0.0.0.0

ISATAP Parameters
Tunnel Local IPv4 address : 0.0.0.0
Router DNS name : ISATAP
Router Solicitation interval : 10 seconds

Robustness : 2
48.1  ip dhcp relay enable (Global)

Use the `ip dhcp relay enable` Global Configuration mode command to enable the DHCP relay feature on the device. Use the `no` form of this command to disable the DHCP relay feature.

**Syntax**

`ip dhcp relay enable`

`no ip dhcp relay enable`

**Parameters**

N/A

**Default Configuration**

DHCP relay feature is disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables the DHCP relay feature on the device.

```conf
switchxxxxxxx(config)# ip dhcp relay enable
```

48.2  ip dhcp relay enable (Interface)

Use the `ip dhcp relay enable` Interface Configuration (VLAN, Ethernet, Port-channel) mode command to enable the DHCP relay feature on an interface. Use the `no` form of this command to disable the DHCP relay agent feature on an interface.
**Syntax**

`ip dhcp relay enable`

`no ip dhcp relay enable`

**Parameters**

N/A

**Default Configuration**

Disabled

**Command Mode**

Interface Configuration (VLAN, Ethernet, Port-channel) mode

**User Guidelines**

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.
  - Or

- DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

**Example**

The following example enables DHCP Relay on VLAN 21.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

### 48.3 `ip dhcp relay address` (Global)

Use the `ip dhcp relay address` Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the `no` form of this command to remove the server from the list.
DHCP Relay Commands

Syntax

ip dhcp relay address ip-address
no ip dhcp relay address [ip-address]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the `no` form of the command with the `ip-address` argument.

The `no` form of the command without the `ip-address` argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

48.4  `ip dhcp relay address` (Interface)

Use the `ip dhcp relay address` Interface Configuration (VLAN, Ethernet, Port-channel) command to define the DHCP servers available by the DHCP relay for DHCP clients connected to the interface. Use the `no` form of this command to remove the server from the list.

Syntax

ip dhcp relay address ip-address
no ip dhcp relay address [ip-address]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Interface Configuration (VLAN, Ethernet, Port-channel) mode

User Guidelines

Use the ip dhcp relay address command to define a DHCP Server IP address per the interface. To define multiple DHCP Servers, use the command multiple times.

Before using this command, set the device to router mode with the command set system.

To remove a DHCP Server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all DHCP servers defined per the interface.

You can use the command regardless if DHCP Relay is enabled on the interface.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

48.5  show ip dhcp relay

Use the show ip dhcp relay EXEC mode command to display the DHCP relay information.

Syntax

show ip dhcp relay
**Command Mode**

**EXEC mode**

**Example**
**Example 1.** Option 82 is not supported:

```bash
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

**Example 2.** Option 82 is supported (disabled):

```bash
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: gi1/1/5, po3-4
  Active:
  Inactive: gi1/1/5, po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active:
  Inactive: 1, 2, 4, 5
Global Servers: 1.1.1.1, 2.2.2.2
```

**Example 3.** Option 82 is supported (enabled):

```bash
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Enabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi1/1/5, po3-4
Active: gi1/1/5
Inactive: po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
Active: 1, 2, 4, 5
Inactive:
Global Servers: 1.1.1.1, 2.2.2.2

Example 3. Option 82 is supported (enabled) and there DHCP Servers defined per interface:

DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi1/1/5, po3-4
Active: gi1/1/5
Inactive: po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
Active: 1, 2, 4, 5
Inactive:
Global Servers: 1.1.1.1, 2.2.2.2
VLAN 1: 1.1.1.1, 100.10.1.1
VLAN 2: 3.3.3.3, 4.4.4.4, 5.5.5.5
VLAN 10: 6.6.6.6
48.6  ip dhcp information option

Use the `ip dhcp information option` Global Configuration command to enable
DHCP option-82 data insertion. Use the `no` form of this command to disable DHCP
option-82 data insertion.

**Syntax**

```
ip dhcp information option
no ip dhcp information option
```

**Parameters**

N/A

**Default Configuration**

DHCP option-82 data insertion is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are
enabled.

**Example**

```
switchxxxxxx(config)# ip dhcp information option
```

48.7  show ip dhcp information option

The `show ip dhcp information option` EXEC mode command displays the DHCP
Option 82 configuration.

**Syntax**

```
show ip dhcp information option
```

**Parameters**

N/A
Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

switchxxxxx# show ip dhcp information option

Relay agent Information option is Enabled
To set the time period during which the authentication key on a key chain is received as valid, use the `accept-lifetime` command in key chain key configuration mode. To revert to the default value, use the `no` form of this command.

**Syntax**

```plaintext
accept-lifetime start-time {infinite | end-time | duration seconds}
no accept-lifetime
```

**Parameters**

- **start-time**—Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following:
  
  ```plaintext
  hh:mm:ss Month date year
  hh:mm:ss date Month year
  
  hh—hours (0-23)
  mm—minutes (0-59)
  ss—seconds (0-59)
  Month—first three letters of the month
  date—date (1-31)
  year—year (four digits)
  
  The default start time and the earliest acceptable date is January 1, 2000.
  ```

- **infinite**—Key is valid to be received from the `start-time` value on.
• **end-time**—Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.

• **duration seconds**—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

### Default Configuration
The default time period during which the authentication key is valid for authenticating incoming packets is set to **Forever**.

The definition of **Forever** is: the starting time is January 1, 2000, and the ending time is infinite.

### Command Mode
Key chain key configuration

### User Guidelines
The switch checks **Time-of-Date** again a value of the *start-time* argument regardless if **Time-of-Date** is not set by management or by SNTP because of the default value of Time-of-Date always is an passed time.

If validation of the value of the *start-time* argument was passed and the *end-time* argument is configured and its value is **infinite** the key is considered as actual regardless if **Time-of-Date** is not set by management or by SNTP.

If **Time-of-Date** is not set by management or by SNTP and if the *end-time* argument is configured with a value differing from **infinite** or the **duration** parameter is configured, the key is considered as expired.

If **Time-of-Date** is set by management or by SNTP, the switch checks **Time-of-Date** again a value of the *end-time* argument or of the **duration** parameter.

If the last key expires, authentication will be finished with error.

### Example
The following example configures a key chain called keychain1. The key named string1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named string2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:
router rip
  network 172.19.1.1
exit
interface ip 172.19.1.1
  ip rip authentication mode md5
  ip rip authentication key-chain keychain1
exit
key chain keychain1
  key 1
    key-string string1
    accept-lifetime 13:30:00 Jan 25 2011 duration 7200
    send-lifetime 14:00:00 Jan 25 2011 duration 3600
  key 2
    key-string string2
    accept-lifetime 14:30:00 Jan 25 2011 duration 7200
    send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit

49.2  ip route

To establish static routes, use the ip route command in global configuration mode. To remove static routes, use the no form of this command.

Syntax

ip route prefix {mask | /prefix-length} {{ip-address [metric cost]}}
no ip route prefix {mask | prefix-length} [ip-address]

Parameters

- prefix—IP route prefix for the destination.
- mask—Prefix mask for the destination.
- /prefix-length—Prefix mask for the destination. Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **ip-address**—IP address of the next hop that can be used to reach that network.
- **reject-route**—Stops routing to the destination network via all gateways.
- **metric cost**—Cost(metric) of the route. The default cost 1. Range: 1–255.

**Default Configuration**

No static routes are established.

**Command Mode**

Global configuration (config)

**User Guidelines**

Use the `no ip route` command without the `ip-address` parameter to remove all static routes to the given subnet.

Use the `no ip route` command with the `ip-address` parameter to remove only one static route to the given subnet via the given next hop.

**Example**

**Example 1**—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

**Example 2**—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length:

```
ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

**Example 3**—The following example shows how to reject packets for network 194.1.1.0:

```
ip route 194.1.1.0 255.255.255.0 reject-route
```
Example 4—The following example shows how to remove all static routes to network 194.1.1.0/24:

```
no ip route 194.1.1.0 /24
```

Example 5—The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
no ip route 194.1.1.0 /24 1.1.1.1
```

### 49.3 ip routing

To enable IP routing, use the `ip routing` command in global configuration mode. To disable IP routing, use the `no` form of this command.

**Syntax**

```
ip routing
no ip routing
```

**Parameters**

This command has no arguments or keywords.

**Default Configuration**

IP routing is disabled.

**Command Mode**

Global configuration (config)

**User Guidelines**

**Example** The following example enables IP routing

```
ip routing
```
### 49.4 key-string

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To specify the authentication string for a key, use the **key-string** command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

**Syntax**

```
key-string text
no key-string
```

**Parameters**

- **text**—Specifies the authentication string. The string can contain from 1 to 16 characters.

**Default Configuration**

No key exists.

**Command Mode**

Key chain key configuration.

**User Guidelines**

**Example**

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
key chain chain1
key 1
```
key-string key1
accept-lifetime 13:30:00 Jan 25 2011 duration 7200
send-lifetime 14:00:00 Jan 25 2011 duration 3600
key 2
key-string key2
accept-lifetime 14:30:00 Jan 25 2011 duration 7200
send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
router rip
network 172.19.1.1
version 2
exit
interface ip 172.19.1.1
ip rip authentication key-chain chain1
ip rip authentication mode md5
exit

49.5  key (key chain)

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To identify an authentication key on a key chain, use the key command in key-chain configuration mode. To remove the key from the key chain, use the no form of this command.

Syntax
key key-id
no key key-id
Parameters

**key-id**—Identification number of an authentication key on a key chain. The range of keys is from 1 to 255. The key identification numbers need not be consecutive. The scope of a key identification number is the key chain where the key is defined.

Default Configuration

No key exists on the key chain.

Command Mode

Key-Chain Configuration mode

User Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the `accept-lifetime` and `send-lifetime` key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will be finished with error.

To remove all keys, remove the key chain by using the `no key chain` command.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
key
key chain chain1
key 1
key-string key1
accept-lifetime 13:30:00 Jan 25 2011 duration 7200
send-lifetime 14:00:00 Jan 25 2011 duration 3600
```
key 2
key-string key2
accept-lifetime 14:30:00 Jan 25 2011 duration 7200
send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
router rip
network 172.19.1.1
exit
interface ip 172.19.1.1
ip rip authentication mode md5
ip rip authentication key-chain chain1
exit

### 49.6 key chain

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To enable authentication for routing protocols, identify a group of authentication keys by using the `key chain` command in global configuration mode. To remove the key chain, use the `no` form of this command.

**Syntax**

```
key chain name-of-chain
no key chain chain-name
```

**Parameters**

- `name-of-chain`—Name of a key chain. The chain-name may have from 1 to 32 characters. A key chain must have at least one key and can have up to 256 keys.

**Default Configuration**

No key chain exists.
Command Mode

Global Configuration mode

User Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the key chain command, you enter **key-chain** configuration mode.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```plaintext
key chain chain1
  key 1
  key-string key1
  accept-lifetime 13:30:00 Jan 25 2011 duration 7200
  send-lifetime 14:00:00 Jan 25 2011 duration 3600
  key 2
  key-string key2
  accept-lifetime 14:30:00 Jan 25 2011 duration 7200
  send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
router rip
  network 172.19.1.1
exit
interface ip 172.19.1.1
  ip rip authentication mode md5
  ip rip authentication key-chain chain1
exit
```
49.7 send-lifetime

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To set the time period during which an authentication key on a key chain is valid to be sent, use the send-lifetime command in key chain key configuration mode. To revert to the default value, use the no form of this command.

Syntax

send-lifetime start-time [infinite | end-time | duration seconds]

no send-lifetime

Parameters

- **start-time**—Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following:

  hh:mm:ss Month date year
  hh:mm:ss date Month year

  *hh*—hours (0-23)
  *mm*—minutes (0-59)
  *ss*—seconds (0-59)

  *Month*—first three letters of the month
  *date*—date (1-31)
  *year*—year (four digits)

  The default start time and the earliest acceptable date is January 1, 2000.

- **infinite**—Key is valid to be received from the *start-time* value on.

- **end-time**—Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
• **duration** *seconds*—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

**Default Configuration**

The default time period during which the authentication key is valid for authenticating incoming packets is set to forever.

**Forever** (the starting time is January 1, 2000, and the ending time is infinite)

**Command Mode**

Key chain key configuration

**User Guidelines**

Specify a *start-time* value and one of the following values: **infinite**, **end-time**, or **duration** *seconds*.

A key is considered as expired if Time-of-Date is not set by management or by SNTP.

If the last key expires, authentication will be finished with error.

**Example**

The following example configures a key chain called chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
router rip
  network 172.19.1.1
exit
interface ip 172.19.1.1
  ip rip authentication mode md5
  ip rip authentication key-chain chain1
exit
key chain chain1
  key 1
```
key-string key1
accept-lifetime 13:30:00 Jan 25 1996 duration 7200
send-lifetime 14:00:00 Jan 25 1996 duration 3600
key 2
key-string key2
accept-lifetime 14:30:00 Jan 25 1996 duration 7200
send-lifetime 15:00:00 Jan 25 1996 duration 3600
exit

49.8 show ip protocols

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To display the parameters and current state of the active IP routing protocol processes, use the show ip protocols command in user EXEC or privileged EXEC mode.

Syntax

show ip protocols [summary]

Parameters

summary—Displays the configured routing protocol process names.

Command Mode

User EXEC
Privileged EXEC

User Guidelines

The information displayed by the show ipv6 protocols command is useful in debugging routing operations.

Example
Example 1. The following is sample output from the `show ip protocols` command, showing active routing protocols:

```
show ip protocols

IP Routing Protocol is "rip"
  Interfaces   IP Addresses
    VLAN 1   12.1.1.1
    VLAN 1   150.23.12.2
    VLAN 11  1.1.1.1

IP Routing Protocol is "ospf 1"
  Interfaces   IP Addresses
    VLAN 3   2.2.2.2
    VLAN 100 154.23.111.1

IPv6 Routing Protocol is "ospf 10"
  Interfaces   IP Addresses
    VLAN 10  123.1.1.1
    VLAN 130 4.4.4.4
```

Example 2. The following is sample output from the `show ip protocols` command with the `summary` keyword:

```
show ipv6 protocols summary

IP Routing Protocol is "rip"
IP Routing Protocol is "ospf 1"
IP Routing Protocol is "ospf 10"
```

49.9  `show ip route`

To display the current state of the routing table, use the `show ip route` command in user EXEC or privileged EXEC mode.
Syntax

```
show ip route [address ip-address {mask [longer-prefixes]} | protocol | static | rejected | icmp | connected]
```

Parameters

- **address ip-address**—IP address about which routing information should be displayed.
- **mask**—The value of the subnet mask.
- **longer-prefixes**—Specifies that only routes matching the IP address and mask pair should be displayed.
- **protocol**—The name of the origin of the protocol to be displayed. Use one of the following arguments:
  - rip—Displays routes added by RIP
  - connected—Displays connected routes.
  - icmp—Displays routes added by ICMP Direct.
  - rejected—Displays rejected routes.
  - static—Displays static routes.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use this command without parameters to display the whole IPv6 Routing table.

Use this command with parameters to specify required routes.

Examples

**Example 1.** The following is sample output from the `show ip route` command when IP Routing is not enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
```
IP Forwarding: disabled

Codes: > - best, C - connected, S - static, I - ICMP

IP Routing Table - 5 entries

<table>
<thead>
<tr>
<th>Code</th>
<th>IP Route</th>
<th>Distance/ Metric</th>
<th>Next Hop</th>
<th>Last Time Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&gt;</td>
<td>10.10.0.0/16</td>
<td>1/128</td>
<td>10.119.254.244</td>
<td>00:02:22 gi1/1/2</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.10.0.0/16</td>
<td>1/128</td>
<td>10.120.254.244</td>
<td>00:02:22 gi1/1/3</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.2.0/24</td>
<td>1/128</td>
<td>10.119.254.244</td>
<td>00:02:22 gi1/1/2</td>
</tr>
<tr>
<td>C&gt;</td>
<td>10.119.0.0/16</td>
<td>0/1</td>
<td>0.0.0.0</td>
<td>gi1/1/2</td>
</tr>
<tr>
<td>C&gt;</td>
<td>10.120.0.0/16</td>
<td>0/1</td>
<td>0.0.0.0</td>
<td>gi1/1/3</td>
</tr>
</tbody>
</table>

Example 2. The following is sample output from the `show ip route` command when IP Routing is enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled
Codes: > - best, C - connected, S - static, R - RIP
IP Routing Table - x entries

<table>
<thead>
<tr>
<th>Code</th>
<th>IP Route</th>
<th>Distance/ Metric</th>
<th>Next Hop</th>
<th>Last Time Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>R&gt;</td>
<td>10.7.10.0/24</td>
<td>120/5</td>
<td>10.119.254.244</td>
<td>00:02:22 gi1/1/2</td>
</tr>
<tr>
<td>C&gt;</td>
<td>10.159.0.0/16</td>
<td>0/1</td>
<td>0.0.0.0</td>
<td>gi1/1/2</td>
</tr>
<tr>
<td>C&gt;</td>
<td>10.170.0.0/16</td>
<td>0/1</td>
<td>0.0.0.0</td>
<td>gi1/1/2</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.175.0.0/16</td>
<td>1/1</td>
<td>10.119.254.240</td>
<td>gi1/1/2</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.180.0.0/16</td>
<td>1/1</td>
<td>10.119.254.240</td>
<td>gi1/1/2</td>
</tr>
</tbody>
</table>
```

Example 3. In the following example, the logical AND operation is performed on the source address 10.16.0.0 and the mask 255.255.0.0, resulting in 10.16.0.0. Each destination in the routing table is also logically ANDed with the mask and
compared to that result of 10.16.0.0. Any destinations that fall into that range are displayed in the output:

```
switchxxxxxx# show ip route 10.16.0.0 255.255.0.0 longer-prefix
```

Maximum Parallel Paths: 1 (1 after reset)

IP Forwarding: enabled

Codes: > - best, C - connected, S - static, R - RIP

IP Routing Table - 6 entries

<table>
<thead>
<tr>
<th>Code</th>
<th>IP Route</th>
<th>Distance/ Metric</th>
<th>Next Hop</th>
<th>Last Time Outgoing</th>
<th>Outgoing Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&gt;</td>
<td>10.16.2.0/24</td>
<td>110/128</td>
<td>10.119.254.244</td>
<td>00:02:22</td>
<td>gi 1/1/2</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.2.64/26</td>
<td>110/128</td>
<td>100.1.14.244</td>
<td>00:02:22</td>
<td>gi 1/1/1</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.2.128/26</td>
<td>110/128</td>
<td>110.9.2.2</td>
<td>00:02:22</td>
<td>gi 1/1/3</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.208.0/24</td>
<td>110/128</td>
<td>120.120.5.44</td>
<td>00:02:22</td>
<td>gi 1/1/2</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.223.0/24</td>
<td>110/128</td>
<td>20.1.2.24</td>
<td>00:02:22</td>
<td>gi 1/1/5</td>
</tr>
<tr>
<td>S&gt;</td>
<td>10.16.236.0/24</td>
<td>110/129</td>
<td>30.19.54.240</td>
<td>00:02:23</td>
<td>gi 1/1/6</td>
</tr>
</tbody>
</table>

### 49.10 show key chain

This command is only relevant for SG500X/SG500XG/ESW2-550X devices.

To display authentication key information, use the `show key chain` command in Privileged EXEC mode.

**Syntax**

```
show key chain [name-of-chain]
```

**Parameters**

- `name-of-chain`—Name of the key chain to display, as named in the key chain command.
**Default Configuration**

Information about all key chains is displayed.

**Command Mode**

Privileged EXEC mode

**Example**

**Example 1.** The following is sample output from the `show key chain` command when the current time or date is defined:

```
switchxxxxxx# show key chain
Current Time of Date is Feb 8 2011
Accept lifetime is configured to ignore
Key-chain trees:
  key 1 -- text "chestnut"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
  key 2 -- text "birch"
    accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)
    send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)[valid now]
```

**Example 2.** The following is sample output from the `show key chain` command when the current time or date is not defined:

```
switchxxxxxx# show key chain
Current Time of Date is not defined
Accept lifetime is ignored
Key-chain trees:
  key 1 -- text "chestnut"
    accept lifetime (always valid) - (always valid) [valid now]
```
send lifetime (always valid) - (always valid) [valid now]

key 2 -- text "birch"

accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)
send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)
ACL Commands

50.1 ip access-list (IP standard)

Use the ip access-list Global Configuration mode command to define an IP standard list. The no format of the command removes the list.

This command is only relevant for SG500X and SG500XG devices.

Syntax

```
ip access-list access-list-name (deny|permit) {src-addr[/src-len] | any}
no ip access-list access-list-name
```

Parameters

- **access-list-name**—The name of the Standard IP access list. The name may contain maximum 32 characters.
- **deny/permit**—Denies/permits access if the conditions are matched.
  - `src-addr[/src-len] | any`—IP prefix defined as an IP address and length or any. The any value matches all IP addresses. If src-len is not defined, a value of 32 is applied. A value of src-len must be in the interval 1-32.

Default Configuration

No access list is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the ip access-list command to configure IP address filtering. Access lists are configured with permit or deny keywords to either permit or deny an IP address based on a matching condition. An implicit deny is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 32.
Evaluation of an IP address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IP address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the **no ip access-list** command to delete the access list.

In addition to filtering IP traffic on a per port base, a basic IP access control list can be used by RIP (Routing Information Protocol) to filter route updates.

**Examples**

**Example 1** - The following example of a standard access list allows only the three specified networks. Any IP address that does not match the access list statements will be rejected.

```plaintext
switchxxxxxx(config)#ip access-list 1 permit 192.168.34.0/24
switchxxxxxx(config)#ip access-list 1 permit 10.88.0.0/16
switchxxxxxx(config)#ip access-list 1 permit 10.0.0.0/8
```

*Note: all other access is implicitly denied.*

**Example 2** - The following example of a standard access list allows access for IP addresses in the range from 10.29.2.64 to 10.29.2.127. All IP addresses not in this range will be rejected.

```plaintext
switchxxxxxx(config)#ip access-list apo permit 10.29.2.64/26
```

*Note: all other access is implicitly denied.*

**Example 3** - To specify a large number of individual addresses more easily, you can omit the mask length if it is 32. Thus, the following two configuration commands are identical in effect:

```plaintext
switchxxxxxx(config)#ip access-list 2aa permit 10.48.0.3
switchxxxxxx(config)#ip access-list 2aa permit 10.48.0.3/32
```

**50.2 ip access-list (IP extended)**

Use the **ip access-list extended** Global Configuration mode command to name an IPv4 access list (ACL) and to place the device in IPv4 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this
ACL are defined in the `permit (IP)` and `deny (IP)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the `no` form of this command to remove the access list.

**Syntax**

```
ip access-list extended acl-name
no ip access-list extended acl-name
```

**Parameters**

- **acl-name**—Name of the IPv4 access list. (Range 1-32 characters)

**Default Configuration**

No IPv4 access list is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

An IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

**Example**

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```

### 50.3 `permit (IP)`

Use the `permit IP` Access-list Configuration mode command to set permit conditions for an IPv4 access list (ACL). Permit conditions are also known as access control entries (ACEs). Use the `no` form of the command to remove the access control entry.

**Syntax**

```
permit protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name]
```
permit icmp \{any / source source-wildcard\} [any / destination destination-wildcard] [any / icmp-type] [any / icmp-code] [dscp number / precedence number] [time-range time-range-name]

permit igmp \{any / source source-wildcard\} [any / destination destination-wildcard] [igmp-type] [dscp number / precedence number] [time-range time-range-name]

permit tcp \{any / source source-wildcard\} [any / source-port/port-range] [any / destination destination-wildcard] [any / destination-port/port-range] [dscp number / precedence number] [match-all list-of-flags] [time-range time-range-name]

permit udp \{any / source source-wildcard\} [any / source-port/port-range] [any / destination destination-wildcard] [any / destination-port/port-range] [dscp number / precedence number] [time-range time-range-name]

no permit protocol \{any / source source-wildcard\} [any / destination destination-wildcard] [dscp number / precedence number] [time-range time-range-name]

no permit icmp \{any / source source-wildcard\} [any / destination destination-wildcard] [any / icmp-type] [any / icmp-code] [dscp number / precedence number] [time-range time-range-name]

no permit igmp \{any / source source-wildcard\} [any / destination destination-wildcard] [igmp-type] [dscp number / precedence number] [time-range time-range-name]

no permit tcp \{any / source source-wildcard\} [any / source-port/port-range] [any / destination destination-wildcard] [any / destination-port/port-range] [dscp number / precedence number] [match-all list-of-flags] [time-range time-range-name]

no permit udp \{any / source source-wildcard\} [any / source-port/port-range] [any / destination destination-wildcard] [any / destination-port/port-range] [dscp number / precedence number] [time-range time-range-name]

Parameters

- **permit protocol**—The name or the number of an IP protocol. Available protocol names are: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the ip keyword. (Range: 0–255)

- **source**—Source IP address of the packet.

- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.

- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.

- **dscp number**—Specifies the DSCP value.

- **precedence number**—Specifies the IP precedence value.

- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535).

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set, it is prefixed by “+”. If a flag should be unset, it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
ACL Commands

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

**Default Configuration**

No IPv4 access list is defined.

**Command Mode**

IP Access-list Configuration mode

**User Guidelines**

- If a range of ports is used for source port in an ACE, it is not counted again, if it is also used for a source port in another ACE. If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

- If a range of ports is used for source port it is counted again if it is also used for destination port.

**Example**

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

**50.4 deny (IP)**

Use the **deny** IP Access-list Configuration mode command to set deny conditions for IPv4 access list. Deny conditions are also known as access control entries (ACEs). Use the no form of the command to remove the access control entry.

**Syntax**

```plaintext
deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name][disable-port ]
deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp number | precedence number] [time-range time-range-name][disable-port ]
deny igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedence number] [time-range time-range-name][disable-port ]
```
deny tcp {any | source source-wildcard} {any | source-port/port-range} {any | destination destination-wildcard} {any | destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port]

deny udp {any | source source-wildcard} {any | source-port/port-range} {any | destination destination-wildcard} {any | destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port]

no deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name] [disable-port]

no deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp number | precedence number] [time-range time-range-name] [disable-port]

no deny igmp {any | source source-wildcard} {any | destination destination-wildcard} [igmp-type] [dscp number | precedence number] [time-range time-range-name] [disable-port]

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igrp, udp, hmp, rdp, idpr, ipv6, ipv6: rout, ipv6: frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the Ip keyword. (Range: 0–255)

- **source**—Source IP address of the packet.

- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.

- **destination**—Destination IP address of the packet.

- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.

- **dscp number**—Specifies the DSCP value.

- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”. If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

- **disable-port**—The Ethernet interface is disabled if the condition is matched.
**Default Configuration**

No IPv4 access list is defined.

**Command Mode**

IP Access-list Configuration mode

**User Guidelines**

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it is counted again if it is also used for destination port.

**Example**

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255 any
```

### 50.5 ipv6 access-list (IPv6 extended)

Use the `ipv6 access-list` Global Configuration mode command to define an IPv6 access list (ACL) and to place the device in IPv6 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit (IPv6)` and `deny (IPv6)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the `no` form of this command to remove the access list.

**Syntax**

```
ipv6 access-list [acl-name]
no ipv6 access-list [acl-name]
```

**Parameters**

- `acl-name`—Name of the IPv6 access list. Range 1-32 characters.

**Default Configuration**

No IPv6 access list is defined.
Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Every IPv6 ACL has an implicit `permit icmp any any nd-ns any, permit icmp any any nd-na any, and deny ipv6 any any` statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process uses the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
Switch (config)# ipv6 access-list acl1
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

50.6  **permit ( IPv6 )**

Use the `permit` command in IPv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

```
permit protocol {any |{source-prefix/length}{any | destination- prefix/length} [dscp number | precedence number] [time-range time-range-name]}
permit icmp {any | {source-prefix/length}{any | destination- prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name]}
permit tcp {any | {source-prefix/length} {any | source-port/port-range}}{any | destination- prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name]
```
**permit udp** {any | {source-prefix/length}} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name]

**no permit** protocol {any |{source-prefix/length}{any | destination-prefix/length} [dscp number | precedence number] [time-range time-range-name]

**no permit icmp** {any | {source-prefix/length}{any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name]

**no permit tcp** {any | {source-prefix/length} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name]

**no permit udp** {any | {source-prefix/length}} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name]

**Parameters**

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **dscp number**—Specifies the DSCP value. (Range: 0–63)
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flag**—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”. If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

**Default Configuration**

No IPv6 access list is defined.

**Command Mode**

Ipv6 Access-list Configuration mode

**User Guidelines**

If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.
Example

This example defines an ACL by the name of server and enters a rule (ACE) for tcp packets.

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

### 50.7 deny (IPv6)

Use the `deny` command in IPv6 Access List Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

**Syntax**

```
deny protocol any [source-prefix/length] any [destination-prefix/length] [dscp number] [precedence number] [time-range time-range-name] [disable-port]
deny icmp any [source-prefix/length] any [destination-prefix/length] [any icmp-type] [any icmp-code] [dscp number] [precedence number] [time-range time-range-name] [disable-port]
deny tcp any [source-prefix/length] [source-port/port-range] any [destination-prefix/length] [any destination-port/port-range] [dscp number] [precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port]
deny udp any [source-prefix/length] [source-port/port-range] any [destination-prefix/length] [any destination-port/port-range] [dscp number] [precedence number] [time-range time-range-name] [disable-port]
no deny protocol any [source-prefix/length] any [destination-prefix/length] [dscp number] [precedence number] [time-range time-range-name] [disable-port]
no deny icmp any [source-prefix/length] any [destination-prefix/length] [any icmp-type] [any icmp-code] [dscp number] [precedence number] [time-range time-range-name] [disable-port]
no deny tcp any [source-prefix/length] any [source-port/port-range] any [destination-prefix/length] any [destination-port/port-range] [dscp number] [precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port]
```

**no deny udp** {any} [source-prefix/length] [any | source-port/port-range] [any | destination-prefix/length] [any | destination-port/port-range] [dscp number | precedence number] [time-range time-range-name] [disable-port]

**Parameters**

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)

- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- **dscp number**—Specifies the DSCP value. (Range: 0–63)

- **precedence number**—Specifies the IP precedence value.

- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), ldap (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), smmp (161), snmptrap (162), sunrpc (111), syslog...
(514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).
(Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.
If a flag should be unset it is prefixed by “-”.
Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

- **disable-port**—The Ethernet interface is disabled if the condition is matched.

**Default Configuration**

No IPv6 access list is defined.

**Command Mode**

IPv6 Access-list Configuration mode

**User Guidelines**

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

**Example**

```bash
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

**50.8 mac access-list**

Use the **mac access-list** Global Configuration mode command to define a Layer 2 access list (ACL) based on source MAC address filtering and to place the device in MAC Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the **permit ( MAC ) and**
deny (MAC) commands. The service-acl input command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax
mac access-list extended acl-name
no mac access-list extended acl-name

Parameters
acl-name—Specifies the name of the MAC ACL (Range: 1–32 characters).

Default Configuration
No MAC access list is defined.

Command Mode
Global Configuration mode

User Guidelines
A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:ff any
```

50.9 permit ( MAC )

Use the permit command in MAC Access List Configuration mode to set permit conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

Syntax
permit [any | source source-wildcard] [any | destination destination-wildcard] [eth-type | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name]

no permit [any | source source-wildcard] [any | destination destination-wildcard] [eth-type | aarp |
**Parameters**

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet. (Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

**Default Configuration**

No MAC access list is defined.

**Command Mode**

MAC Access-list Configuration mode

**Example**

```plaintext
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:ff any
```

**50.10 deny (MAC)**

Use the **deny** command in MAC Access List Configuration mode to set deny conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.
Syntax

deny {any | source source-wildcard} {any | destination destination-wildcard} 
[ {eth-type} | arpa | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000]
[_vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port ]

no deny {any | source source-wildcard} {any | destination destination-wildcard} 
[ {eth-type} | arpa | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000]
[_vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port ]

Parameters

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094).
- **cos**—The Class of Service of the packet. (Range: 0–7).
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

Example

```bash
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:ff any
```
50.11 service-acl input

Use the service-acl input command in interface Configuration mode to bind an access list(s) (ACL) to an interface.

Use the no form of this command to remove all ACLs from the interface.

Syntax

```
service-acl input acl-name1 [acl-name2] [default-action {deny-any | permit-any}]
no service-acl input
```

Parameters

- **acl-name**—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- **deny-any**—Deny all packets (that were ingress at the port) that do not meet the rules in this ACL.
- **permit-any**—Forward all packets (that were ingress at the port) that do not meet the rules in this ACL.

Default Configuration

No ACL is assigned.

Command Mode

Interface Configuration (Ethernet, Port-Channel, VLAN) mode

User Guidelines

The following rules govern when ACLs can be bound or unbound from an interface:

- IPv4 ACLs and IPv6 ACLs can be bound together to an interface.
- A MAC ACL cannot be bound on an interface which already has an IPv4 ACL or IPv6 ACL bound to it.
- Two ACLs of the same type cannot be bound to a port.
- An ACL cannot be bound to a port that is already bound to an ACL, without first removing the current ACL. Both ACLs must be mentioned at the same time in this command.
- MAC ACLs that include a VLAN as match criteria cannot be bound to a VLAN.
- ACLs with time-based configuration on one of its ACEs cannot be bound to a VLAN.
- ACLs with the action Shutdown cannot be bound to a VLAN.
- When the user binds ACL to an interface, TCAM resources will be consumed. One TCAM rule for each MAC or IP ACE and two TCAM rules for each IPv6 ACE. TCAM consumption is always an even number, so when an odd number of rules is used, consumption is increased by 1.

Example

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

50.12 time-range

Use the time-range Global Configuration mode command to define time ranges for functions or ACLs. In addition, this command enters the Time-range Configuration mode. All commands after this one refer to the time-range being defined.

This command sets a time-range name. Use the absolute and periodic commands to actually configure the time-range.

Use the no form of this command to remove the time range from the device.

Syntax

```
time-range time-range-name
no time-range time-range-name
```

Parameters

- `time-range-name`—Specifies the name for the time range. (Range: 1–32 characters)
Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After adding the name of a time range with this command, use the absolute and periodic commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bound to any features.

When a time range is defined, it can be used in the following commands:

- dot1x port-control
- power inline
- permit (IP)
- deny (IP)
- permit (IPv6)
- deny (IPv6)
- permit (MAC)
- deny (MAC)

Example

```
switchxxxxxx(config)# time-range http-allowed

console(config-time-range)# periodic mon 12:00 to wed 12:00
```
50.13  absolute

Use the absolute Time-range Configuration mode command to specify an absolute time when a time range is in effect. Use the no form of this command to remove the time limitation.

Syntax

```
absolute start hh:mm day month year
no absolute start
absolute end hh:mm day month year
no absolute end
```

Parameters

- **start**—Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- **end**—Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- **hh:mm**—Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- **day**—Day (by date) in the month. (Range: 1–31)
- **month**—Month (first three letters by name). (Range: Jan...Dec)
- **year**—Year (no abbreviation) (Range: 2000–2097)

Default Configuration

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

Example

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```
50.14 periodic

Use the periodic Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the no form of this command to remove the time limitation.

Syntax

periodic day-of-the-week hh:mm to day-of-the-week hh:mm

no periodic day-of-the-week hh:mm to day-of-the-week hh:mm

periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]

no periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]

periodic list hh:mm to hh:mm all

no periodic list hh:mm to hh:mm all

Parameters

- **day-of-the-week**—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines). Possible values are: mon, tue, wed, thu, fri, sat, and sun.

- **hh:mm**—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)

- **list day-of-the-week1**—Specifies a list of days that the time range is in effect.

Default Configuration

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode
User Guidelines

The second occurrence of the day can be at the following week, e.g. Thursday–Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00

50.15 show time-range

Use the show time-range EXEC command to display the time range configuration.

Syntax

show time-range time-range-name

Parameters

time-range-name—Specifies the name of an existing time range.

Command Mode

EXEC mode

Example

switchxxxxxx# show time-range
http-allowed

----------------

absolute start 12:00 1 Jan 2005 end 12:00 31 Dec 2005
periodic Monday 12:00 to Wednesday 12:00

50.16 show access-lists

Use the show access-lists Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.
Syntax

show access-lists [name]
show access-lists time-range-active [name]

Parameters

- **name**—Specifies the name of the ACL.
- **time-range-active**—Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

switchxxxxxx# show access-lists
Standard IP access list 1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any time-range weekdays

switchxxxxxx# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays

switchxxxxxx# show access-lists ACL1
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any
50.17  show interfaces access-lists

Use the `show interfaces access-lists` Privileged EXEC mode command to display access lists (ACLs) applied on interfaces.

Syntax

```
show interfaces access-lists [interface-id]
```

Parameters

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

```
show interfaces access-lists

Interface            ACLs
---------            -------------
        gi1/1/1      blockcdp, blockvtp
        gi1/1/2            Ingress: server1
                           Egress : ip
```
Quality of Service (QoS) Commands

51.1 qos

Use the `qos` Global Configuration mode command to enable QoS on the device and set its mode. Use the `no` form of this command to disable QoS on the device.

Syntax

```
qos [basic | advanced [ports-not-trusted | ports-trusted]]

no qos
```

Parameters

- **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.

- **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.

- **ports-not-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to egress queue 0. This is the default setting in advanced mode.

- **ports-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to an egress queue based on the packet's fields. Use the `qos advanced-mode trust` command to specify the trust mode.

Default Configuration

If `qos` is entered without any keywords, the QoS `basic` mode is enabled.

If `qos advanced` is entered without a keyword, the default is `ports-not-trusted`.

Command Mode

Global Configuration mode
Examples

Example 1 - The following example enables QoS basic mode on the device.

```
switchxxxxxx(config)# qos
```

Example 2 - The following example enables QoS advanced mode on the device with the `ports-not-trusted` option.

```
switchxxxxxx(config)# qos advanced
```

51.2 qos advanced-mode trust

Use the `qos advanced-mode trust` Global Configuration command to configure the trust mode in advanced mode. Use the `no` form of this command to return to default.

Syntax

```
qos advanced-mode trust {cos | dscp | cos-dscp}
```

```
oqos advanced-mode trust
```

Parameters

- `cos`—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- `dscp`—Classifies ingress packets with the packet DSCP values.
- `cos-dscp`—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

Default Configuration

```
cos-dscp
```

Command Mode

Global Configuration

User Guidelines

The configuration is relevant for advanced mode in the following cases:
• **ports-not-trusted mode**: For packets that are classified to the QoS action trust.

• **ports-trusted mode**: For packets that are not classified by to any QoS action or classified to the QoS action trust.

**Example**

The following example sets cos as the trust mode for QoS on the device.

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

### 51.3 show qos

Use the `show qos` EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

**Syntax**

```
show qos
```

**Parameters**

N/A

**Default Configuration**

Disabled Command Mode

**Command Mode**

EXEC mode

**User Guidelines**

Trust mode is displayed if QoS is enabled in basic mode.

**Examples**

**Example 1** - The following example displays QoS attributes when QoS is enabled in basic mode and the advanced mode is supported.

```
switchxxxxxx# show qos
```
Example 2 - The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is not supported.

switchxxxxxx# show qos
Qos: disable
Trust: dscp

51.4 class-map

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally-named service policy applied on a per-interface basis.

A class map consists of one or more ACLs (see ACL Commands). It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

Use the class-map Global Configuration mode command to create or modify a class map and enter the Class-map Configuration mode (only possible when QoS is in the advanced mode).

Use the no form of this command to delete a class map.

All class map commands are only available when QoS is in advanced mode.

Syntax

class-map class-map-name [match-all | match-any]

no class-map class-map-name

Parameters

- class-map-name—Specifies the class map name.
- match-all—Performs a logical AND of all the criteria of the ACLs belonging to this class map. All match criteria in this class map must be matched.
- match-any—Performs a logical OR of the criteria of the ACLs belonging to this class map. Only a single match criteria in this class map must be matched.
**Default Configuration**

If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

The **class-map** enters Class-map Configuration mode. In this mode, up to two **match** commands can be entered to configure the criteria for this class. Each **match** specifies an ACL.

When using two **match** commands, each must point to a different type of ACL, such as: one IP ACL and one MAC ACL. The classification is by first match, therefore, the order of the ACLs is important.

Error messages are generated in the following cases:

- There is more than one **match** command in a **match-all** class map
- There is a repetitive classification field in the participating ACLs.

After entering the Class-map Configuration mode, the following configuration commands are available:

- **exit**: Exits the Class-map Configuration mode.
- **match**: Configures classification criteria.
- **no**: Removes a match statement from a class map.

**Example**

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the ACL specified.

```
switchxxxxxx(config)# class-map class1 match-all
switchxxxxxx(config-cmap)#match access-group acl-name
```

**51.5 show class-map**

The **show class-map** EXEC mode command displays all class maps when QoS is in advanced mode.
Syntax

show class-map [class-map-name]

Parameters

class-map-name—Specifies the name of the class map to be displayed.

Command Mode

EXEC mode

Example

The following example displays the class map for Class1.

```
switchxxxxxx# show class-map
Class Map matchAny class1
    Match access-group mac
```

51.6 match

Use the match Class-map Configuration mode command to bind the ACLs that belong to the class-map being configured. Use the no form of this command to delete the ACLs.

This command is available only when the device is in QoS advanced mode.

Syntax

match access-group acl-name

no match access-group acl-name

Parameters

acl-name—Specifies the MAC or IP ACL name.

Default Configuration

No match criterion is supported.

Command Mode

Class-map Configuration mode.
Example
The following example defines a class map called Class1. Class1 contains an ACL called enterprise. Only traffic matching all criteria in enterprise belong to the class map.

```plaintext
switchxxxxxx(config)# class-map class1
switchxxxxxx(config-cmap)# match access-group enterprise
```

51.7 policy-map
A policy map contains one or more class maps and an action that is taken if the packet matches the class map. Policy maps may be bound to ports/port-channels.

Use the `policy-map` Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the `no` form of this command to delete a policy map.

This command is only available when QoS is in advanced mode.

Syntax
```
policy-map policy-map-name

no policy-map policy-map-name
```

Parameters

`policy-map-name`—Specifies the policy map name.

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
Use the `policy-map` Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

Entering the `policy-map` Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a
policy map can be configured only if the classes have match criteria defined for them.

Policy map is applied on the ingress path.

The match criteria is for a class map. Only one policy map per interface is supported. The same policy map can be applied to multiple interfaces and directions.

The `service-policy` command binds a policy map to a port/port-channel.

**Example**

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```plaintext
switchxxxxxx(config)# policy-map policy1
```

```plaintext
switchxxxxxx(config-pmap)#
```

---

### 51.8 **class**

Use the `class` Policy-map Configuration mode command after the `policy-map` command to attach ACLs to a policy-map.

Use the `no` form of this command to detach a class map from a policy map.

This command is only available when QoS is in advanced mode.

**Syntax**

```plaintext
class class-map-name [access-group acl-name]
no class class-map-name
```

**Parameters**

- `class-map-name`—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name.

- `access-group acl-name`—Specifies the name of an IP or MAC Access Control List (ACL).

**Default Configuration**

No class map is defined for the policy map.
**Command Mode**

Policy-map Configuration mode

**User Guidelines**

This is the same as creating a class map and then binding it to the policy map.

You can specify an existing class map in this command, or you can use the `access-group` parameter to create a new class map.

After the policy-map is defined, use the `service-policy` command to attach it to a port/port-channel.

**Example**

The following example defines a traffic classification (class map) called `class1` containing an ACL called `enterprise`. The class is in a policy map called `policy1`. The policy-map `policy1` now contains the ACL `enterprise`.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1 access-group enterprise
```

### 51.9 show policy-map

Use the `show policy-map` EXEC mode command to display all policy maps or a specific policy map.

This command is only available when QoS is in advanced mode.

**Syntax**

```
show policy-map [policy-map-name]
```

**Parameters**

`policy-map-name`—Specifies the policy map name.

**Default Configuration**

All policy-maps are displayed.

**Command Mode**

EXEC mode
Example
The following example displays all policy maps.

```
switchxxxxxx# show policy-map
Policy Map policy1
class class1
set IP dscp 7
Policy Map policy2
class class2
police 96000 4800 exceed-action drop
class class3
police 124000 96000 exceed-action policed-dscp-transmit
```

51.10 trust
Use the trust Policy-map Class Configuration mode command to configure the trust state. This command is relevant only when QoS is in advanced, ports-not-trusted mode. Trust indicates that traffic is sent to the queue according to the packet’s QoS parameters (UP or DSCP).

Use the no form of this command to return to the default trust state.

This command is only available when QoS is in advanced mode.

Syntax
```
trust
no trust
```

Parameters
N/A

Default Configuration
The default state is according to the mode selected in the qos command (advanced mode). The type of trust is determined in qos advanced-mode trust.
**Command Mode**

Policy-map Class Configuration mode

**User Guidelines**

Use this command to distinguish the QoS trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

The type of trust is determined in `qos advanced-mode trust`.

Trust values set with this command supersede trust values set on specific interfaces with the `qos trust (Interface)` Interface Configuration mode command.

The `trust` and `set` commands are mutually exclusive within the same policy map.

Policy maps, which contain `set` or `trust` commands or that have ACL classification to an egress interface, cannot be attached by using the `service-policy` Interface Configuration mode command.

If specifying `trust cos`, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

**Example**

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state using the DSCP value in the ingress packet.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map cl
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map pl
switchxxxxxx(config-pmap)# class cl
switchxxxxxx(config-pmap-c)# trust cos-dscp
```
51.11 set

Use the **set** Policy-map Class Configuration mode command to select the value that QoS uses as the DSCP value, the egress queue or to set user priority values. This command is only available when QoS is in advanced mode.

**Syntax**

```
set {dscp new-dscp | queue queue-id | cos new-cos}
no set
```

**Parameters**

- **dscp new-dscp**—Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- **queue queue-id**—Specifies the egress queue. (Range: 1-8)
- **cos new-cos**—Specifies the new user priority to be marked in the packet. (Range: 0–7)

**Command Mode**

Policy-map Class Configuration mode

**User Guidelines**

The **set** and **trust** commands are mutually exclusive within the same policy map.

To return to the Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

**Example**

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in the policy map called p1.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map cl
switchxxxxxx(config-cmap)# match access-group ip1
```
51.12 police

Use the `police` Policy-map Class Configuration mode command to define the policer for classified traffic. This defines another group of actions for the policy map (per class map).

This command is used after the `policy-map` and `class` commands.

Use the `no` form of this command to remove a policer.

This command is only available when QoS is in advanced mode.

Syntax

```
police committed-rate-kbps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]  
```

```
no police  
```

Parameters

- `committed-rate-kbps`—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 100–10000000)

- `committed-burst-byte`—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)

- `exceed-action {drop | policed-dscp-transmit}`—Specifies the action taken when the rate is exceeded. The possible values are:
  - `drop`—Drops the packet.
  - `policed-dscp-transmit`—Remarks the packet DSCP according to the policed-DSCP map as configured by the `qos map policed-dscp` Global Configuration mode command.

Default Usage

N/A
**Command Mode**

Policy-map Class Configuration mode

**User Guidelines**

This command only exists in when the device is in Layer 2 mode.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

**Example**

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps and the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action drop
```

**51.13 service-policy**

Use the `service-policy` Interface Configuration (Ethernet, Port-channel) mode command to bind a policy map to a port/port-channel. Use the `no` form of this command to detach a policy map from an interface.

This command is only available in QoS advanced mode.

**Syntax**

```
service-policy input policy-map-name default-action [permit-any | deny-any]
no service-policy input
```

**Parameters**

- **policy-map-name**—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)
- **deny-any**—Deny all the packets (which were ingress of the port) that do not meet the rules in a policy.
- **permit-any**—Forward all the packets (which were ingress of the port) that do not meet the rules in a policy.
Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Default
deny-any

User Guidelines
Only one policy map per interface per direction is supported.

Example
Example 1—The following example attaches a policy map called Policy1 to the input interface.

```
switchxxxxxx(config-if)# service-policy input policy1
```

Example 2—The following example attaches a policy map called Policy1 to the input interface and forwards all packets that do not meet the rules of the policy.

```
switchxxxxxx(config-if)# service-policy input policy1 permit-any
```

51.14 qos aggregate-policer
Use the qos aggregate-policer Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the no form of this command to remove an existing aggregate policer.

This command is only available when QoS is in advanced mode.

Syntax
```
qos aggregate-policer aggregate-policer-name committed-rate-kbps excess-burst-byte [exceed-action {drop | policed-dscp-transmit}]
```

```
no qos aggregate-policer aggregate-policer-name
```

Parameters
- aggregate-policer-name—Specifies the aggregate policer name.
Quality of Service (QoS) Commands

- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–57982058)
- **excess-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action** [{drop} | **policed-dscp-transmit** ]—Specifies the action taken when the rate is exceeded. The possible values are:
  - `drop`—Drops the packet.
  - `policed-dscp-transmit`—Remarks the packet DSCP.

**Default Configuration**

No aggregate policer is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command only exists when the device is in Layer 2.

Define an aggregate policer if the policer aggregates traffic from multiple class maps.

Aggregate policers cannot aggregate traffic from multiple devices. If the aggregate policer is applied to more than one device, the traffic on each device is counted separately and is limited per device.

Traffic from two different ports on the same device can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

**Example**

The following example defines the parameters of a policer called Policer1 that can be applied to multiple classes in the same policy map. When the average traffic
rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600
 exceed-action drop
```

### 51.15  show qos aggregate-policer

Use the `show qos aggregate-policer` EXEC mode command to display aggregate policers.

This command is only available in QoS advanced mode.

**Syntax**

```
show qos aggregate-policer [aggregate-policer-name]
```

**Parameters**

- `aggregate-policer-name`—Specifies the aggregate policer name.

**Default Configuration**

All policers are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the parameters of the aggregate policer called Policer1.

```
switchxxxxxx#  show qos aggregate-policer policer1
 aggregate-policer policer1 96000 4800 exceed-action drop
 not used by any policy map
```
51.16 police aggregate

Use the **police aggregate** Policy-map Class Configuration mode command to apply an aggregate policer to multiple class maps within the same policy map. Use the **no** form of this command to remove an existing aggregate policer from a policy map.

This command is only available in QoS advanced mode.

**Syntax**

```plaintext
police aggregate aggregate-policer-name
no police aggregate aggregate-policer-name
```

**Parameters**

- **aggregate-policer-name**—Specifies the aggregate policer name.

**Command Mode**

Policy-map Class Configuration mode

**User Guidelines**

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the **exit** command to return to the Configuration mode. Use the **end** command to return to the Privileged EXEC mode.

**Example**

The following example applies the aggregate policer called Policer1 to a class called class1 in a policy map called policy1 and class2 in policy map policy2.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600
exceed-action drop
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police aggregate policer1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
```
51.17  

**wrr-queue cos-map**

Use the `wrr-queue cos-map` Global Configuration mode command to map Class of Service (CoS) values to a specific egress queue. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
wrr-queue cos-map queue-id cos0... cos7
no wrr-queue cos-map [queue-id]
```

**Parameters**

- `queue-id` — Specifies the queue number to which the CoS values are mapped.
- `cos0... cos7` — Specifies up to 8 CoS values to map to the specified queue number. (Range: 0–7)

**Default Configuration**

The default CoS value mapping to 8 queues is as follows:

CoS value 0 is mapped to queue 1.
CoS value 1 is mapped to queue 2.
CoS value 2 is mapped to queue 3.
CoS value 3 is mapped to queue 6.
CoS value 4 is mapped to queue 5.
CoS value 5 is mapped to queue 8.
CoS value 6 is mapped to queue 8.
CoS value 7 is mapped to queue 7.

The default CoS value mapping to 4 queues is as follows:

CoS value 0 is mapped to queue 1.
CoS value 1 is mapped to queue 1.
CoS value 2 is mapped to queue 2.
CoS value 3 is mapped to queue 3.
CoS value 4 is mapped to queue 3.
CoS value 5 is mapped to queue 4.
CoS value 6 is mapped to queue 4.
CoS value 7 is mapped to queue 4.

Command Mode
Global Configuration mode

User Guidelines
Use this command to distribute traffic to different queues.

Example
The following example maps CoS value 4 and 6 to queue 2.

```plaintext
switchxxxxxx(config)# wrr-queue cos-map 2 4 6
```

51.18  wrr-queue bandwidth

Use the `wrr-queue bandwidth` global Configuration command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the `no` form of this command to restore the default configuration.

Syntax

`wrr-queue bandwidth weight1 weight2... weighting`
`no wrr-queue bandwidth`

Parameters

`weight1 weight1... weighting` the ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. See explanation in the User Guidelines. Separate each value by a space. (Range for each weight: 0–255)
Default Configuration

wrr is disabled by default. The default wrr weight is ‘1’ for all queues.

Command Mode

Global Configuration mode

User Guidelines

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite queue is a priority queue, which is serviced until empty before the other queues are serviced. The expedite queues are designated by the priority-queue out num-of-queues command.

Example

The following assigns WRR values to the queues.

```
switchxxxxx(config)#priority-queue out num-of-queues 0
switchxxxxx(config)#wrr-queue bandwidth 6 6 6
```

51.19 priority-queue out num-of-queues

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

Use the priority-queue out num-of-queues Global Configuration mode command to configure the number of expedite queues. Use the no form of this command to restore the default configuration.

Syntax

```
priority-queue out num-of-queues number-of-queues
```
no priority-queue out num-of-queues

Parameters

- **number-of-queues**—Specifies the number of expedite (strict priority) queues. Expedite queues are assigned to the queues with the higher indexes. (Range: 0–8).
  
  There must be either 0 wrr queues or more than one.

- If **number-of-queues** = 0, all queues are assured forwarding (according to wrr weights). If the **number-of-queues** = 8, all queues are expedited (strict priority queues).
  
  Note: the maximum number of queues depends on the value set in the **set system** command.

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

the weighted round robin (WRR) weight ratios are affected by the number of expedited queues, because there are fewer queues participating in WRR. This indicates that the corresponding weight in the **wrr-queue bandwidth** Interface Configuration mode command is ignored (not used in the ratio calculation).

Example

The following example configures the number of expedite queues as 2.

```
switchxxxxxxx(config)# priority-queue out num-of-queues 2
```

51.20 **traffic-shape**

The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Use the **traffic-shape** Interface Configuration mode command to configure the egress port shaper. Use the **no** form of this command to disable the shaper.
Syntax

traffic-shape committed-rate [committed-burst]

no traffic-shape

Parameters

- **committed-rate**—Specifies the maximum average traffic rate (CIR) in kbits per second (kbps). (Range: FE, GE: 64kbps–maximum port speed; 10GE: 64Kbps–maximum port speed)

- **committed-burst**—Specifies the maximum permitted excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example sets a traffic shaper on gi1/1/5 when the average traffic rate exceeds 64 kbps or the normal burst size exceeds 4096 bytes.

switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# traffic-shape 64 4096

51.21 traffic-shape queue

The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Use the **traffic-shape queue** Interface Configuration mode command to configure the egress queue shaper. Use the **no** form of this command to disable the shaper.

Syntax

```plaintext
traffic-shape queue queue-id committed-rate [committed-burst]

no traffic-shape queue queue-id
```
Parameters

- **queue-id**—Specifies the queue number to which the shaper is assigned. (Range: 1-8). Note: the maximum number of queues depends on the value set in the `set system` command.

  - **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)

  - **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example sets a shaper on queue 1 on gi1/1/5 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# traffic-shape queue 1 64 4096
```

51.22 rate-limit (Ethernet)

Use the `rate-limit` Interface Configuration mode command to limit the incoming traffic rate on a port. Use the `no` form of this command to disable the rate limit.

Syntax

```
rate-limit committed-rate-kbps [burst committed-burst-bytes]
no rate-limit
```

Parameters

- **committed-rate-kbps**—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 100–max port speed.
**burst committed-burst-bytes**—The burst size in bytes (3000–19173960). If unspecified, defaults to 128K.

**Default Configuration**
Rate limiting is disabled.
Committed-burst-bytes is 128K.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**
Storm control and rate-limit (of Unicast packets) cannot be enabled simultaneously on the same port.

**Example**
The following example limits the incoming traffic rate on gi1/1/5 to 150,000 kbps.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# rate-limit 150000
```

### 51.23  rate-limit (VLAN)
Use the Layer 2 rate-limit (VLAN) Global Configuration mode command to limit the incoming traffic rate for a VLAN. Use the no form of this command to disable the rate limit.

**Syntax**

```
rate-limit vlan-id committed-rate committed-burst
no rate-limit vlan
```

**Parameters**

- **vlan-id**—Specifies the VLAN ID.
- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3-57982058)
Quality of Service (QoS) Commands

- **committed-burst**—Specifies the maximum burst size (CBS) in bytes. (Range: 3000-19173960)

**Default Configuration**
Rate limiting is disabled.
Committed-burst-bytes is 128K.

**Command Mode**
Global Configuration mode

**User Guidelines**
The rate limit is calculated separately for each unit in a stack, and for each packet processor in a unit.

Traffic policing in a policy map takes precedence over VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

This command does not work in Layer 3 mode. It does not work in conjunction with IP Source Guard.

**Example**
The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.

```
switchxxxxxx(config)# rate-limit 11 150000 9600
```

51.24 **qos wrr-queue wrtd**

Use the `qos wrr-queue wrtd` Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the `no` form of this command to disable WRTD.

**Syntax**

```
qos wrr-queue wrtd
no qos wrr-queue wrtd
```
Parameters
N/A

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
The command is effective after reset.

Example

```
switchxxxxxx(conf)#> qos wrr-queue wrtd
This setting will take effect only after copying running configuration to startup configuration and resetting the device
```

```
switchxxxxxx(config)#
```

### 51.25  `show qos wrr-queue wrtd`

Use the `show qos wrr-queue wrtd` Exec mode command to display the Weighted Random Tail Drop (WRTD) configuration.

**Syntax**

```
show qos wrr-queue wrtd
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Exec mode
Example

```
switchxxxxxx# show qos wrr-queue wrtd
Weighted Random Tail Drop is disabled
Weighted Random Tail Drop will be enabled after reset
```

51.26 show qos interface

Use the `show qos interface` EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

```
show qos interface [buffers / queueing / policers / shapers / rate-limit] [interface-id]
```

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the 8 queues. For FE ports, this displays the minimum reserved setting.
- **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused (on a VLAN).
- **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **rate-limit**—Displays the rate-limit configuration.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

Default Configuration

N/A

Command Mode

EXEC mode
User Guidelines

If no parameter is specified with the `show qos interface` command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP-map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Examples

**Example 1** - This is an example of the output from the `show qos interface queueing` command for 4 queues.

Ethernet gi0/1

wrr bandwidth weights and EF priority:

<table>
<thead>
<tr>
<th>qid-weights</th>
<th>Ef - Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - N/A</td>
<td>ena- 1</td>
</tr>
<tr>
<td>2 - N/A</td>
<td>ena- 2</td>
</tr>
<tr>
<td>3 - N/A</td>
<td>ena- 3</td>
</tr>
<tr>
<td>4 - N/A</td>
<td>ena- 4</td>
</tr>
</tbody>
</table>

Cos-queue map:

<table>
<thead>
<tr>
<th>cos-qid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 1</td>
</tr>
<tr>
<td>1 - 1</td>
</tr>
<tr>
<td>2 - 2</td>
</tr>
<tr>
<td>3 - 3</td>
</tr>
<tr>
<td>4 - 3</td>
</tr>
<tr>
<td>5 - 4</td>
</tr>
<tr>
<td>6 - 4</td>
</tr>
<tr>
<td>7 - 4</td>
</tr>
</tbody>
</table>
Example 1 - This is an example of the output from the `show qos interface buffers` command for 8 queues.

```
switchxxxxxx# show qos interface buffers gi1/1/1

Notify Q depth:
buffers gi1/1/1
Ethernet gi1/1/1

<table>
<thead>
<tr>
<th>qid</th>
<th>thresh0</th>
<th>thresh1</th>
<th>thresh2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>2</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>3</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>7</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>8</td>
<td>100</td>
<td>100</td>
<td>80</td>
</tr>
</tbody>
</table>
```
Example 2 - This is an example of the output from the `show qos interface shapers` command.

```
switchxxxxxx# show qos interface shapers gi1/1/1

Port shaper: enable

Committed rate: 192000 bps

Committed burst: 9600 bytes

<table>
<thead>
<tr>
<th>QID</th>
<th>Status</th>
<th>Target Committed Rate [bps]</th>
<th>Target Committed Burst [bytes]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>100000</td>
<td>17000</td>
</tr>
<tr>
<td>2</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>Enable</td>
<td>200000</td>
<td>19000</td>
</tr>
<tr>
<td>4</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Enable</td>
<td>178000</td>
<td>8000</td>
</tr>
<tr>
<td>8</td>
<td>Enable</td>
<td>23000</td>
<td>1000</td>
</tr>
</tbody>
</table>
```
Example - 3 This is an example of the output from `show qos interface policer`

```bash
switchxxxxxx# show qos interface policer gi1/1/1
Ethernet gi1/1/1
Class map: A
Policer type: aggregate
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: drop
Class map: C
Policer type: none
Commited rate: N/A
Commited burst: N/A
Exceed-action: N/A
```

Example 4 - This is an example of the output from `show qos interface rate-limit`

```
console#show qos interface rate-limit gi0/1

Port    rate-limit [kbps]  Burst [Bytes]
-------- ----------------- --------------
      gi0/1          3000            3000
```

Example 5 - This is an example of the output from `show qos interface rate-limit`

```
 switchxxxxxx# show qos interface rate-limit gi1/1/1
 Port      rate-limit [kbps]  Burst [Bytes]
 ----- ----------------- --------------
    gi1/1/1       1000            512
```

51.27 qos map policed-dscp

Use the `qos map policed-dscp` Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the `no` form of this command to restore the default configuration.

This command is only available in QoS advanced mode.
Syntax

qos map policed-dscp  dscp-list  to  dscp-mark-down
no qos map policed-dscp [dscp-list]

Parameters

- **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- **dscp-mark-down**—Specifies the DSCP value to mark down. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

The original DSCP value and policed-DSCP value must be mapped to the same queue in order to prevent reordering.

Example

The following example marks incoming DSCP value 3 as DSCP value 5 on the policed-DSCP map.

```
switchxxxxxx(config)# qos map policed-dscp 3 to 5
```

51.28  qos map dscp-queue

Use the qos map dscp-queue Global Configuration mode command to configure the DSCP to CoS map. Use the no form of this command to restore the default configuration.

Syntax

qos map dscp-queue  dscp-list  to  queue-id
no qos map dscp-queue [dscp-list]
Parameters

- **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- **queue-id**—Specifies the queue number to which the DSCP values are mapped.

**Default Configuration**

The default map for 4 queues is as follows.

<table>
<thead>
<tr>
<th>DSCP value</th>
<th>0-15</th>
<th>16-23</th>
<th>24-39,48-63</th>
<th>40-47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue-ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

The default map for 8 queues is as follows.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue-ID</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration mode

**Example**

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
switchxxxxxx(config)# qos map dscp-queue 33 40 41 to 1
```

51.29  **qos trust (Global)**

Use the **qos trust** Global Configuration mode command to configure the system to the basic mode and trust state. Use the **no** form of this command to return to the default configuration.

**Syntax**

```
qos trust {cos/dscp}
```

```
no qos trust
```
Parameters

- **cos**—Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp**—Specifies that ingress packets are classified with packet DSCP values.

Default Configuration

DSCP is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

This command can be used only in QoS basic mode.

Packets entering a QoS domain are classified at its edge. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

For an inter-QoS domain boundary, configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different in the QoS domains.

Example

The following example configures the system to the DSCP trust state.

```
switchxxxxxx(config)# qos trust dscp
```
51.30  qos trust (Interface)

Use the qos trust Interface Configuration (Ethernet, Port-channel) mode command to enable port trust state while the system is in the basic QoS mode. Use the no form of this command to disable the trust state on each port.

Syntax
qos trust
no qos trust

Parameters
N/A

Default Configuration
Each port is enabled while the system is in basic mode.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example configures gi1/1/15 to the default trust state.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# qos trust
```

51.31  qos cos

Use the qos cos Interface Configuration (Ethernet, Port-channel) mode command to define the default CoS value of a port. Use the no form of this command to restore the default configuration.

Syntax
qos cos default-cos
no qos cos
Parameters

default-cos—Specifies the default CoS value (VPT value) of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

Default Configuration

The default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

Example

The following example defines the port gi1/1/5 default CoS value as 3.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# qos cos 3
```

### 51.32 qos dscp-mutation

Use the `qos dscp-mutation` Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the `no` form of this command to restore the trusted port with no DSCP mutation.

Syntax

```
qos dscp-mutation

no qos dscp-mutation
```

Parameters

N/A

Default Configuration

Disabled
Command Mode

Global Configuration mode.

User Guidelines

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port.

Global trust mode must be DSCP or CoS-DSCP. In advanced CoS mode, ports must be trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
switchxxxxxx(config)# qos dscp-mutation
```

51.33  qos map dscp-mutation

Use the `qos map dscp-mutation` Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the `no` form of this command to restore the default configuration.

Syntax

```
qos map dscp-mutation in-dscp to out-dscp
no qos map dscp-mutation [in-dscp]
```

Parameters

- **in-dscp**—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- **out-dscp**—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)
Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
switchxxxxxxx(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

51.34 show qos map

Use the `show qos map` EXEC mode command to display the various types of QoS mapping.

Syntax

```
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]
```

Parameters

- `dscp-queue`—Displays the DSCP to queue map.
- `dscp-dp`—Displays the DSCP to Drop Precedence map.
- `policed-dscp`—Displays the DSCP to DSCP remark table.
- `dscp-mutation`—Displays the DSCP-DSCP mutation table.

Default Configuration

Display all maps.
**Command Mode**

EXEC mode

**Example**

The following example displays the QoS mapping information:

```
Sx500-L2#show qos map dscp-queue
Dscp-queue map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-------------------------------------
  0 : 01 01 01 01 01 01 01 01 01 01
  1 : 01 01 01 01 01 01 02 02 02 02
  2 : 02 02 02 03 03 03 03 03 03 03
  3 : 03 03 03 03 03 03 03 03 03 03
  4 : 04 04 04 04 04 04 04 04 03 03
  5 : 03 03 03 03 03 03 03 03 03 03
  6 : 03 03 03 03
```

**51.35 clear qos statistics**

Use the `clear qos statistics` EXEC mode command to clear the QoS statistics counters.

**Syntax**

```
clear qos statistics
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode
Example
The following example clears the QoS statistics counters.

```
switchxxxxxx# clear qos statistics
```

51.36 qos statistics policer

Use the `qos statistics policer` Interface Configuration (Ethernet, Port-channel) mode command to enable counting in-profile and out-of-profile. Use the `no` form of this command to disable counting.

This command is relevant only when policers are defined.

Syntax

```
qos statistics policer policy-map-name class-map-name

no qos statistics policer policy-map-name class-map-name
```

Parameters

- `policy-map-name`—Specifies the policy map name.
- `class-map-name`—Specifies the class map name.

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
console(config)#interface gi1/1/1

switchxxxxxx(config-if)# qos statistics policer policy1 class1
```
51.37  qos statistics aggregate-policer

Use the `qos statistics aggregate-policer` Global Configuration mode command to enable counting in-profile and out-of-profile. Use the `no` form of this command to disable counting.

Syntax

```
qos statistics aggregate-policer aggregate-policer-name
no qos statistics aggregate-policer aggregate-policer-name
```

Parameters

- `aggregate-policer-name`—Specifies the aggregate policer name.

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Global Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# qos statistics aggregate-policer policer1
```

51.38  qos statistics queues

Use the `qos statistics queues` Global Configuration mode command to enable QoS statistics for output queues. Use the `no` form of this command to disable QoS statistics for output queues.

Syntax

```
qos statistics queues set {queue | all} {dp | all} {interface | all}
no qos statistics queues set
```

Parameters

- `queue`—Specifies a specific output queue.
- `all`—Specifies all output queues.
- `dp`—Specifies the output queue for packets with DSCP.
- `all`—Specifies all output queues with DSCP.
- `interface`—Specifies a specific output interface.
- `all`—Specifies all output interfaces.

Default Configuration

QoS statistics for output queues are disabled.

Command Mode

Global Configuration mode
Parameters

- **set**—Specifies the counter set number.
- **interface**—Specifies the Ethernet port.
- **queue**—Specifies the output queue number.
- **dp**—Specifies the drop precedence. The available values are: `high`, `low`.

Default Configuration

Set 1: All interfaces, all queues, high DP.
Set 2: All interfaces, all queues, low DP.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

If the queue parameter is all, traffic in stacking and cascading ports is also counted.

Example

The following example enables QoS statistics for output queues for counter set 1.

```plaintext
switchxxxxxx(config)# qos statistics queues 1 all all all
```

51.39  **show qos statistics**

Use the `show qos statistics` EXEC mode command to display Quality of Service statistical information.

Syntax

```plaintext
show qos statistics
```

Parameters

N/A
Default Configuration
N/A

Command Mode
EXEC mode

User Guidelines
Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the `qos statistics queues` Global Configuration mode command to enable QoS statistics for output queues.

Example
The following example displays Quality of Service statistical information.

```
switchxxxxxx# show qos statistics
Policers
--------
Interface Policy map Class In-profile bytes Out-of-profile bytes
-------- ------- ------ --------------- ---------------
---------- ------- ------ --------------- ---------------
gi1/1/1 Policy1 Class1 7564575 52
      Policy1 Class2 8759 3214
      Policy1 Class1 746587458 23
      Policy1 Class2 5326
Aggregate Policers
------------------
Name In-profile bytes Out-of-profile bytes
------- --------------- ---------------
Policer1 7985687 121322

Output Queues
------------
Interface Queue DP Total packets TD packets
------- ----- -- ------------- --------------
gi1/1/1 2 High 799921 1.2%
gi1/1/2 All High 5387326 0.2%
```
Denial of Service (DoS) Commands

52.1 security-suite deny syn-fin

Use the `security-suite deny syn-fin` Global Configuration mode command to drop all ingressing TCP packets in which both SYN and FIN are set.

Use the `no` form of this command to permit TCP packets in which both SYN and FIN are set.

**Syntax**

```
security-suite deny syn-fin
no security-suite deny syn-fin
```

**Default Configuration**

The feature is disabled by default.

**Command Mode**

Global Configuration mode

**Example**

The following example blocks TCP packets in which both SYN and FIN flags are set.

```
switchxxxxxx(config)# security-suite deny sin-fin
```

52.2 security-suite syn protection mode

Use the `security-suite syn protection mode` Global Configuration mode command to set the TCP SYN protection mode.

Use the `no` form of this command to set the TCP SYN protection mode to default.

**Syntax**

```
For security-suite syn protection mode {disabled | report | block}
```
no security-suite syn protection mode

Parameters

- **disabled**—Feature is disabled
- **report**—Feature reports about TCP SYN traffic per port (including rate-limited SYSLOG message when an attack is identified)
- **block**—TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited SYSLOG message (one per minute) is generated

Default Configuration
The default mode is block.

Command Mode
Global Configuration mode

User Guidelines
On ports in which an ACL is defined (user-defined ACL etc.), this feature cannot block TCP SYN packets. In case the protection mode is block but SYN Traffic cannot be blocked, a relevant SYSLOG message will be created, e.g.: “port gi1/1/1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.”

Examples

**Example 1:** The following example sets the TCP SYN protection feature to report TCP SYN attack on ports in case an attack is identified from these ports.

```plaintext
switchxxxxxx(config)# security-suite syn protection mode report
...
01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port gi1/1/1
```

**Example 2:** The following example sets the TCP SYN protection feature to block TCP SYN attack on ports in case an attack is identified from these ports.

```plaintext
switchxxxxxx(config)# security-suite syn protection mode block
...
01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port gi1/1/1. TCP SYN traffic destined to the local system is automatically blocked for 100 seconds.
```
52.3  security-suite syn protection threshold

Use the `security-suite syn protection threshold` Global Configuration mode command to set the threshold for the SYN protection feature. Use the `no` form of this command to set the threshold to its default value.

**Syntax**

```
security-suite syn protection threshold syn-packet-rate
no security-suite syn protection threshold
```

**Parameters**

- `syn-packet-rate`—defines the rate (number of packets per second) from each specific port that triggers identification of TCP SYN attack. (Range: 20-200)

**Default Configuration**

The default threshold is 80pps (packets per second).

**Command Mode**

Global Configuration mode

**Example**

The following example sets the TCP SYN protection threshold to 40 pps.

```
switchxxxxx(config)# security-suite syn protection threshold 40
```

52.4  security-suite syn protection recovery

Use the `security-suite syn protection period` Global Configuration mode command to set the time period for the SYN Protection feature to block an attacked interface. Use the `no` form of this command to set the time period to its default value.

**Syntax**

```
security-suite syn protection recovery timeout
no security-suite syn protection recovery
```

**Parameters**

- `timeout`—defines the timeout (in seconds) by which an interface from which SYN packets are blocked gets unblocked. Note that if a SYN attack is still active on this interface it might become blocked again. (Range: 10-600)
Default Configuration
The default timeout is 60 seconds.

Command Mode
Global Configuration mode

User Guidelines
If the timeout is modified, the new value will be used only on interfaces which are not currently under attack.

Example
The following example sets the TCP SYN period to 100 seconds.

```
switchxxxxxxx(config)# security-suite syn protection recovery 100
```

52.5 show security-suite syn protection

Use the `show security-suite syn protection` EXEC mode command to display the SYN Protection feature configuration and the operational status per interface-id, including the time of the last attack per interface.

Syntax

```
show security-suite syn protection [interface-id]
```

Parameters

- `interface-id`—Specifies an interface-ID. The interface-ID can be one of the following types: Ethernet port of Port-Channel.

Command Mode
EXEC mode

User Guidelines
Use the Interface-ID to display information on a specific interface.

Example
The following example displays the TCP SYN protection feature configuration and current status on all interfaces. In this example, port gi1/1/2 is attacked but since there is a user-ACL on this port, it cannot become blocked so its status is `Reported` and not `Blocked and Reported`.

```
switchxxxxxxx# show security-suite syn protection
```
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>Current Status</th>
<th>Last Attack Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>151</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012 Blocked and Reported</td>
</tr>
<tr>
<td>152</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012 Reported</td>
</tr>
<tr>
<td>153</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012 Blocked and Reported</td>
</tr>
</tbody>
</table>

52.6 security-suite enable

Use the `security-suite enable` Global Configuration mode command to enable the security suite feature. This feature supports protection against various types of attacks.

When this command is used, hardware resources are reserved. These hardware resources are released when the `no security-suite enable` command is entered.

The security-suite feature can be enabled in one of the following ways:

- **Global-rules-only**—This enables the feature globally but per-interface features are not enabled.
- **All (no keyword)**—The feature is enabled globally and per-interface.

Use the `no` form of this command to disable the security suite feature.

When security-suite is enabled, you can specify the types of protection required. The following commands can be used:

- `security-suite dos protect`
- `security-suite dos syn-attack`
- `security-suite deny martian-addresses`
- `security-suite deny syn`
- `security-suite deny icmp`
- `security-suite deny fragmented`
- `show security-suite configuration`
- `security-suite dos protect`
Denial of Service (DoS) Commands

Syntax

security-suite enable [global-rules-only]

no security-suite enable

Parameters

global-rules-only—Specifies that all the security suite commands are global commands only (they cannot be applied per-interface). This setting saves space in the Ternary Content Addressable Memory (TCAM). If this keyword is not used, security-suite commands can be used both globally on per-interface.

Default Configuration

The security suite feature is disabled.

If global-rules-only is not specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

MAC ACLs must be removed before the security-suite is enabled. The rules can be re-entered after the security-suite is enabled.

If ACLs or policy maps are assigned on interfaces, per interface security-suite rules cannot be enabled.

Examples

Example 1—The following example enables the security suite feature and specifies that security suite commands are global commands only. When an attempt is made to configure security-suite on a port, it fails.

switchxxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxxx(config)# interface gi1
switchxxxxxxx(config-if)# security-suite dos syn-attack 199 any /10

To perform this command, DoS Prevention must be enabled in the per-interface mode.

Example 2—The following example enables the security suite feature globally and on interfaces. The security-suite command succeeds on the port.
52.7 security-suite dos protect

Use the `security-suite dos protect` Global Configuration mode command to protect the system from specific well-known Denial of Service (DoS) attacks. There are three types of attacks against which protection can be supplied (see parameters below).

Use the `no` form of this command to disable DoS protection.

**Syntax**

`security-suite dos protect [add attack | remove attack]`

`no security-suite dos protect`

**Parameters**

`add/remove attack`—Specifies the attack type to add/remove. To add an attack is to provide protection against it; to remove the attack is to remove protection.

The possible attack types are:

- `stacheldraht`—Discards TCP packets with source TCP port 16660.
- `invasor-trojan`—Discards TCP packets with destination TCP port 2140 and source TCP port 1024.
- `back-orifice-trojan`—Discards UDP packets with destination UDP port 31337 and source UDP port 1024.

**Default Configuration**

No protection is configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

For this command to work, `security-suite enable` must be enabled globally.
Example
The following example protects the system from the Invasor Trojan DOS attack.

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

52.8 security-suite dos syn-attack

Use the `security-suite dos syn-attack` Interface Configuration mode command to rate limit Denial of Service (DoS) SYN attacks. This provides partial blocking of SYN packets (up to the rate that the user specifies).

Use the `no` form of this command to disable rate limiting.

Note: This feature is only supported when the device is in Layer 2 switch mode.

Syntax

```
security-suite dos syn-attack syn-rate {any | ip-address} {mask | /prefix-length}
no security-suite dos syn-attack {any | ip-address} {mask | /prefix-length}
```

Parameters

- `syn-rate`—Specifies the maximum number of connections per second. (Range: 199–1000)
- `any | ip-address`—Specifies the destination IP address. Use `any` to specify all IP addresses.
- `mask`—Specifies the network mask of the destination IP address.
- `prefix-length`—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

No rate limit is configured.

If `ip-address` is unspecified, the default is 255.255.255.255

If `prefix-length` is unspecified, the default is 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode
User Guidelines

For this command to work, `security-suite enable` must be enabled both globally and for interfaces.

This command rate limits ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses.

SYN attack rate limiting is implemented after the security suite rules are applied to the packets. The ACL and QoS rules are not applied to those packets.

Since the hardware rate limiting counts bytes, it is assumed that the size of “SYN” packets is short.

Example

The following example attempts to rate limit DoS SYN attacks on a port. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

52.9  `security-suite deny martian-addresses`

Use the `security-suite deny martian-addresses` Global Configuration mode command to deny packets containing system-reserved IP addresses or user-defined IP addresses.

Syntax

```
security-suite deny martian-addresses [add {ip-address [mask | /prefix-length]} | remove {ip-address [mask | /prefix-length]}] (Add/remove user-specified IP addresses)

security-suite deny martian-addresses reserved [add / remove] (Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses (This command removes addresses reserved by security-suite deny martian-addresses [add {ip-address [mask | /prefix-length]} | remove {ip-address [mask | /prefix-length]}], and removes all entries added by the user. The user can remove a specific entry by using remove ip-address [mask | /prefix-length] parameter.
```
There is no form of the `security-suite deny martian-addresses reserved [add | remove]` command. Use instead the `security-suite deny martian-addresses reserved remove` command to remove protection (and free up hardware resources).

**Parameters**

- **reserved add/remove**—Add or remove the table of reserved addresses below.
- **ip-address**—Adds/discards packets with the specified IP source or destination address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).
- **reserved**—Discards packets with the source or destination IP address in the block of the reserved (Martian) IP addresses. See the User Guidelines for a list of reserved addresses.

**Default Configuration**

Martian addresses are allowed.

**Command Mode**

Global Configuration mode

**User Guidelines**

For this command to work, `security-suite enable` must be enabled globally.

`security-suite deny martian-addresses reserved` adds or removes the addresses in the following table:

<table>
<thead>
<tr>
<th>Address block</th>
<th>Present Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/8 (except when 0.0.0.0/32 is the source address)</td>
<td>Addresses in this block refer to source hosts on “this’ network.</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>This block is assigned for use as the Internet host loopback address.</td>
</tr>
<tr>
<td>192.0.2.0/24</td>
<td>This block is assigned as “TEST-NET” for use in documentation and example code.</td>
</tr>
</tbody>
</table>
Denial of Service (DoS) Commands

Note that if the reserved addresses are included, individual reserved addresses cannot be removed.

Example

The following example discards all packets with a source or destination address in the block of the reserved IP addresses.

switchxxxxxx(config)# security-suite deny martian-addresses reserved add

52.10 security-suite deny syn

Use the `security-suite deny syn` Interface Configuration (Ethernet, Port-channel) mode command to block the creation of TCP connections from a specific interface. This a complete block of these connections.

Use the `no` form of this command to permit creation of TCP connections.

Syntax

```
security-suite deny syn {[add [tcp-port / any] [ip-address / any] [mask /prefix-length]] /
[remove [tcp-port / any] [ip-address / any] [mask /prefix-length]]}
```

Parameters

- `ip-address | any`—Specifies the destination IP address. Use `any` to specify all IP addresses.
- `mask`—Specifies the network mask of the destination IP address.
- `prefix-length`—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (`/`).

<table>
<thead>
<tr>
<th>Address block</th>
<th>Present Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0/4 as source</td>
<td>This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.</td>
</tr>
<tr>
<td>240.0.0.0/4 (except when 255.255.255.255/3 2 is the destination address)</td>
<td>This block, formerly known as the Class E address space, is reserved.</td>
</tr>
</tbody>
</table>
Denial of Service (DoS) Commands

- `tcp-port | any`—Specifies the destination TCP port. The possible values are: `http`, `ftp-control`, `ftp-data`, `ssh`, `telnet`, `smtp`, or `port number`. Use `any` to specify all ports.

**Default Configuration**

Creation of TCP connections is allowed from all interfaces.

If the `mask` is not specified, it defaults to `255.255.255.255`.

If the `prefix-length` is not specified, it defaults to `32`.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

For this command to work, `security-suite enable` must be enabled both globally and for interfaces.

The blocking of TCP connection creation from an interface is done by discarding ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses and destination TCP ports.

**Example**

The following example attempts to block the creation of TCP connections from an interface. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

**52.11 security-suite deny icmp**

Use the `security-suite deny icmp` Interface Configuration (Ethernet, Port-channel) mode command to discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network).

Use the `no` form of this command to permit echo requests.
Syntax

security-suite deny icmp {add {ip-address | any} [mask /prefix-length]] | [remove {ip-address | any} [mask /prefix-length]]

no security-suite deny icmp

Parameters

- **ip-address | any**—Specifies the destination IP address. Use any to specify all IP addresses.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Echo requests are allowed from all interfaces.

If **mask** is not specified, it defaults to 255.255.255.255.

If **prefix-length** is not specified, it defaults to 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

For this command to work, **security-suite enable** must be enabled both globally and for interfaces.

This command discards ICMP packets with "ICMP type= Echo request" that ingress the specified interface.

Example

The following example attempts to discard echo requests from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.
52.12 security-suite deny fragmented

Use the `security-suite deny fragmented` Interface Configuration (Ethernet, Port-channel) mode command to discard IP fragmented packets from a specific interface.

Use the `no` form of this command to permit IP fragmented packets.

Syntax

```
security-suite deny fragmented {
  [add {ip-address | any} {mask | /prefix-length}] |
  [remove {ip-address | any} {mask | /prefix-length}]
}

no security-suite deny fragmented
```

Parameters

- `ip-address | any`—Specifies the destination IP address. Use `any` to specify all IP addresses.
- `mask`—Specifies the network mask of the IP address.
- `prefix-length`—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Fragmented packets are allowed from all interfaces.

If `mask` is unspecified, the default is 255.255.255.255.

If `prefix-length` is unspecified, the default is 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

For this command to work, `security-suite enable` must be enabled both globally and for interfaces.

Example

The following example attempts to discard IP fragmented packets from an interface.
Denial of Service (DoS) Commands

switchxxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxxx(config)# interface gi1
switchxxxxxxx(config-if)# security-suite deny fragmented add any /32

To perform this command, DoS Prevention must be enabled in the per-interface mode.

52.13 show security-suite configuration

Use the `show security-suite configuration` EXEC mode command to display the security-suite configuration.

**Syntax**

`show security-suite configuration`

**Command Mode**

EXEC mode

**Example**

The following example displays the security-suite configuration.

```
switchxxxxxxx# show security-suite configuration
Security suite is enabled (Per interface rules are enabled).
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack
Interface                      IP Address      SYN Rate (pps)
------------------------------------------------------------------
gi1/1/1                       176.16.23.0\24   100
Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering
Interface                      IP Address      TCP port
------------------------------------------------------------------
gi1/1/2                       176.16.23.0\24   FTP
```

ICMP filtering
### Fragmented packets filtering

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/1/2</td>
<td>176.16.23.0/24</td>
</tr>
<tr>
<td>gi1/1/2s</td>
<td>176.16.23.0/24</td>
</tr>
</tbody>
</table>
VRRP Commands

53.1 clear vrrp counters

The clear vrrp counters Privileged EXEC mode command clears the VRRP counters.

Syntax

clear vrrp counters [interface-id]

Parameters

interface-id—Interface Identifier.

Default Configuration

No description.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command without the identifier-id argument, to clear the VRRP counters of all interfaces where Virtual routers are running.

Use this command with the identifier-id argument, to clear the VRRP counters of the specified interface.
Example

The following example shows how to clear the counters of all VRRP Virtual routers running on VLAN 10:

clear vrrp counters vlan10

53.2 show vrrp

The `show vrrp` Privileged EXEC mode command displays a brief or detailed status of one or all configured VRRP virtual routers.

Syntax

`show vrrp [all | brief | interface interface-id]`

Parameters

- `all`—Provides VRRP virtual router information about all VRRP virtual routers, including virtual routers in a disable status.
- `brief`—Provides a summary view of the VRRP virtual router information
- `interface interface-id`—Interface identifier

Command Mode

Privileged EXEC mode

Example 1.

`show vrrp`

Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10(down)
Source IP address is 10.3.0.20 is down; a default Source IP address of 10.2.0.10 is applied
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.20 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec

Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.20, 10.5.0.20
Source IP address is 10.4.0.20 (default)
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
Master Router is 10.4.0.20 (local), priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 1.000 sec

Interface: VLAN 50
Virtual Router 1
Supported version is VRRPv3
State is Backup
Virtual Router name CLUSTER3
Virtual IP addresses are 10.6.0.10
Source IP address is 10.6.0.20 (default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.6.0.10, priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 0.628 sec

Interface VLAN 400
Virtual Router 4
Supported version is VRRPv3
State is Initializing
Virtual Router name CLUSTER4
Virtual IP addresses are 10.7.0.10
Source IP address is 10.7.0.20
Virtual MAC address is 00:00:5e:00:01:03
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150

Example 2.

```
show vrrp interface vlan10
```
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10
Source IP address is 10.3.0.20
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.10 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec
Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.10, 10.5.0.10
Source IP address is 10.4.0.10
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.4.0.10 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec

Example 3.
```
show vrrp brief
```
State (S): I - Initialize; M - Master; B - Backup
Preempt (P): Y - Yes; N - No

<table>
<thead>
<tr>
<th>Interface VR</th>
<th>Virtual</th>
<th>Pri</th>
<th>Timer</th>
<th>P</th>
<th>St</th>
<th>Ver</th>
<th>Source address</th>
<th>Master address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge1/0/24</td>
<td>254</td>
<td>254</td>
<td>40000</td>
<td>Y</td>
<td>M</td>
<td>2</td>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>VLAN 10</td>
<td>1</td>
<td>100</td>
<td>3000</td>
<td>Y</td>
<td>M</td>
<td>3</td>
<td>10.3.0.10</td>
<td>10.3.0.10</td>
</tr>
<tr>
<td>VLAN 10</td>
<td>2</td>
<td>255</td>
<td>1000</td>
<td>Y</td>
<td>M</td>
<td>3</td>
<td>10.4.0.10</td>
<td>10.4.0.10</td>
</tr>
<tr>
<td>VLAN 50</td>
<td>1</td>
<td>95</td>
<td>1000</td>
<td>Y</td>
<td>B</td>
<td>3</td>
<td>10.6.0.10</td>
<td>10.6.0.60</td>
</tr>
<tr>
<td>VLAN 400</td>
<td>4</td>
<td>150</td>
<td>1000</td>
<td>Y</td>
<td>I</td>
<td>3</td>
<td>10.7.0.10</td>
<td></td>
</tr>
</tbody>
</table>

53.3 show vrrp counters

The `show vrrp counters` Privileged EXEC mode command displays the VRRP counters.
**Syntax**

`show vrrp counters [interface-id]`

**Parameters**

`interface-id`—Interface Identifier.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use the `show vrrp counters` command without the `interface-id` argument, to display the VRRP counters of all interfaces where Virtual routers are running.

Use the `show vrrp counters` command with the `interface-id` argument, to display the VRRP counters of the specified interface.

**Example**

The following example display the counters of all Virtual routers defined on VLAN 100:

```
show vrrp counters vlan 100
vlan 100
Invalid checksum: 0
Invalid Packet Length: 0
Invalid TTL: 0
Invalid VRRP Packet Type: 0
Invalid VRRP ID: 0
Invalid Protocol Number: 0
Invalid IP List: 0
Invalid Interval: 0
Invalid Authentication: 0
```
53.4 vrrp description

The `vrrp description` Interface Configuration mode command assigns a description to the VRRP virtual router. The `no` format of the command returns to the default.

**Syntax**

```
vrrp vrid description text
no vrrp vrid description
```

**Parameters**

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `text`—Text that describes the purpose or use of the virtual router. The parameter may contain 0-160 characters.

**Default Configuration**

No description.

**Command Mode**

Ethernet port, LAG, VLAN

**Example**

The following example shows how to assign a VRRP description to specified VRRP virtual router

```
interface vlan 10
  vrrp 1 description router1
exit
```

53.5 vrrp ip

The `vrrp ip` Interface Configuration mode command defines an IP address of a virtual router. The `no` format of the command removes an IP address.
Syntax

```
vrrp vrid ip ip-address
no vrrp vrid ip [ip-address]
```

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

- **ip-address**—Virtual router's IP address.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

A virtual router comes into existence when it has one or more participating VRRP routers. To participate in a specific virtual router as a VRRP router, use `vrrp ip` to configure an existing IP interface with the identifier and the IP address(es) of the virtual router. The IP interface of the VRRP router and the virtual router must be in the same IP subnet.

A VRRP router that is the owner if the virtual router's IP address(es) is also the VRRP router real IP address at the IP interface. There is only one owner for all virtual router's IP address(es). A VRRP router participates in a virtual router when it is configured with the first virtual router's IP address and does not participate when the virtual router IP address is removed.

A virtual router entity in a VRRP router is created in the shutdown state. Use the `no vrrp shutdown` command to enable it.

To defined more than one virtual router's IP address, the command should be applied for each configured IP address.

Each VRRP router in the virtual router should be configured with the same set of IP addresses.

If the **ip-address** parameter is omitted in the `no` format of the CLI command, all the IP addresses of the virtual router are remove, leading to the virtual router entity in the VRRP router being removed too.

Example

The following example shows how to define a VRRP virtual router
interface vlan 10
  vrrp 1 ip 192.168.2.1
exit

53.6 vrrp preempt

The vrrp preempt Interface Configuration mode command enables Virtual Router Redundancy Protocol (VRRP) preemption. The no format of the command disables the preemption.

Syntax

vrrp vrid preempt
no vrrp vrid preempt

Parameters

vrid—Virtual router identifier the interface for which VRRP is being defined. The range is 1-255.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

Preemption is enabled by default.

User Guidelines

By default, the VRRP router being configured with this command will take over as Master virtual router for the group if it has a higher priority than the current master virtual router.

Note: The router that is the IP address owner will preempt, regardless of the setting of this command.

Example

The following example shows how to disable VRRP preemption to specified VRRP virtual router

interface vlan 10
no vrrp 1 preempt

exit

53.7  vrrp priority

The vrrp priority Interface Configuration mode command defines Virtual Router Redundancy Protocol (VRRP) priority. The no format of the command returns to the default.

Syntax

vrrp  vrid  priority  priority

no vrrp  vrid  priority

Parameters

- vrid—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- priority—Virtual router priority. The range is 1-254.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

The default for owner is 255 and for non-owner it is 100.

User Guidelines

The priority of the owner cannot be changed. It is always 255.

Example

The following example shows how to set VRRP priority:

```
interface  vlan  10
   vrrp  1  priority  110
exit
```
53.8 vrrp shutdown

The `vrrp shutdown` Interface Configuration mode command disables the VRRP virtual router on the interface (meaning that it changes its status to Initialize). The `no` format of the command enables the VRRP virtual router.

**Syntax**

```
vrrp vrid shutdown
no vrrp vrid shutdown
```

**Parameters**

`vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

**Default Configuration**

Disabled.

**Command Mode**

Ethernet port, LAG, VLAN

**User Guidelines**

When a VRRP virtual router is disabled on an interface its configuration is not removed.

**Example**

The following example shows how to enable a specified virtual router

```
interface vlan 10
  no vrrp 1 shutdown
exit
```

53.9 vrrp source-ip

The `vrrp source-ip` Interface Configuration mode command defines a real VRRP address that will be used as the source IP address of VRRP messages. The `no` format of the command returns to the default.
Syntax

vrrp  vrid  source-ip  ip-address
no  vrrp  vrid source-ip

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **ip-address**—VRRP router's IP address: one of IP addresses of VRRP router defined on the same interface.

Default Configuration

Lowest VRRP router's IP address defined on the interface.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

Example

The following example shows how to define source ip address to specified VRRP virtual router

```
interface vlan 10
  vrrp 1 source-ip 192.168.2.1
exit
```

53.10  vrrp timers advertise

The **vrrp timers advertise** Interface Configuration mode command defines the interval between successive advertisements by the Master VRRP virtual router. The **no** format of the command returns to the default.

Syntax

vrrp  vrid timers advertise [msec] interval
no  vrrp  vrid timers advertise
Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **msec**—Changes the unit of the advertisement time from seconds to milliseconds. Without the keyword, the advertisement interval is in seconds.
- **interval**—Time interval between successive advertisements. If keyword `msec` is present then the valid range is 50 to 40950 milliseconds. If keyword `msec` is omitted then the valid range is 1 to 40 seconds.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

1 second

User Guidelines

If the advertisement interval is configured in msec, the operation advertisement interval will be the configured advertisement interval round down to the nearest seconds for VRRP v2 and to the nearest centiseconds (10ms) for VRRP v3.

Example

The following example shows how to set VRRP timer advertise of 500 msec to specified VRRP virtual router:

```bash
interface vlan 10
  vrrp 1 timers advertise msec 500
exit
```

53.11 vrrp version

The `vrrp version` Interface Configuration mode command defines the supported VRRP version. The no format of the command returns to the default.

Syntax

```
vrrp vrid version 2 | 3 | 2&3
```
no vrrp vrid version

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **2**—VRRPv2 specified by RFC3768 is supported. Received VRRPv3 messages are dropped by the VRRP virtual router. Only VRRPv2 advertisements are sent.
- **3**—VRRPv3 specified by RFC5798 is supported without VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are dropped by the VRRP virtual router. Only VRRPv3 advertisements are sent.
- **2&3**—VRRPv3 specified by RFC5798 is supported with VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are treated by the VRRP virtual router. VRRPv3 and VRRPv2 advertisements are sent.

Default Configuration

Version 2.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

Version 2&3 is intended for upgrade scenarios and is not for permanent deployment. Please refer to VRRP 3 standard for version 2 and version 3 interoperability.

Example

The following example shows how to define VRRP version to specified VRRP virtual router

```plaintext
interface vlan 10
  vrrp 1 version 2
exit
```
54.1 clear rip statistics

The clear rip statistics Privileged EXEC mode command clears statistics counters of all interfaces and all peers.

Syntax

clear rip statistics

Parameters

N/A

Default Configuration

Command Mode

Privileged EXEC

User Guidelines

Example

The following example shows how to clear all counters:

```
clear rip statistics
```

54.2 default-information originate

To generate a default route into Routing Information Protocol (RIP), use the default-information originate command in Router Configuration mode. To disable this feature, use the no form of this command.

Syntax

default-information originate

no default-information originate
**Default Configuration**

Default route is not generated by RIP.

**Command Mode**

Router configuration (config-router).

**Examples**

**Example 1** - The following example shows the result of using this command in Router RIP mode:

```console
switch065500(config)#router rip
switch065500(config-rip)#default-information originate
switch065500#sh ip rip database
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: 1
Redistributing is disabled
```

**Example 2** - The following example shows the result of using this command in Interface mode:

```console
switch065500(config-rip)#interface ip 1.1.1.1
switch065500(config-ip)#ip rip default-information originate 14
switch065500#sh ip rip database
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: 1
Redistributing is disabled
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 1
Default Originate Metric is 14
```
No Authentication
No IN Filtering
No OUT Filtering

54.3 default-metric

The default-metric Router RIP configuration mode command sets the default metric value when RIP advertises routes derived by other protocols (for example, by static configuration). The no format of the command sets the default value.

Syntax

```
default-metric [metric-value]
no default-metric
```

Parameters

- **metric-value**—Default metric value. Range 1-15.

Default Configuration

```
metric-value—1.
```

Command Mode

Router RIP configuration.

User Guidelines

Example

The following example shows how to set the default metric to 2:

```
router rip
  default-metric 2
exit
```
54.4  ip rip authentication key-chain

The **ip rip authentication key-chain** IP Interface Configuration mode command specifies the set of keys that can be used for and specifies the type of authentication. The **no** format of the command returns to default.

**Syntax**

```
ip rip authentication key-chain name-of-chain
no ip rip authentication key-chain
```

**Parameters**

*name-of-chain*—Specifies the name of key set. The name-change parameter points to list of keys specified by the **key chain** CLI command.

**Default Configuration**

No defined key chain.

**Command Mode**

IP interface mode

**User Guidelines**

Use the **ip rip authentication key-chain** IP Interface Configuration mode command to define a key chain name. Only one key chain may be defined per an IP interface. Each the **ip rip authentication key-chain** command overrides the previous definition.

In order to have a smooth rollover of keys in a key chain, a key should be configured with a lifetime that starts several minutes before the lifetime of the previous key expires.

**Example**

The following example shows how to define a chain name:

```
interface ip 1.1.1.1
   ip rip authentication key-chain alpha
exit
```
54.5  ip rip authentication mode

The `ip rip authentication mode` IP Interface Configuration mode command enables authentication. The `no` format of the command returns to default.

**Syntax**

```
ip rip authentication mode {text | md5}
no ip rip authentication mode
```

**Parameters**

- `text`—Specifies the clear text authentication.
- `md5`—Specifies the MD5 authentication.

**Default Configuration**

No authentication.

**Command Mode**

IP interface mode

**User Guidelines**

If you enable the MD5 authentication, you must configure a key chain name with the `ip rip authentication key-chain` interface command. If a key chain is not defined for the IP interface or there is not a valid key then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the clear text authentication, you must configure a password with the `ip rip authentication-key` interface command. If a password is not defined for the IP interface then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

**Example**

The following example shows how to set the md5 mode:

```
interface ip 1.1.1.1
  ip rip authentication mode md5
exit
```
54.6  ip rip authentication-key

To assign a password to be used by neighboring routers that are using the RIP clear text authentication, use the `ip rip authentication-key` command in interface configuration mode. To remove a previously assigned RIP password, use the `no` form of this command.

Syntax

```
ip rip authentication-key password
no ip rip authentication-key
```

Parameters

`password`—Any continuous string of characters that can be entered from the keyboard up to 8 characters in length.

Default Configuration

No password is specified.

Command Mode

IP interface mode

User Guidelines

The password created by this command is used as a "key" that is inserted directly into the RIP header when the switch software originates routing protocol packets. A separate password can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same password to be able to exchange RIP information.

Only one password may be defined per an IP interface. Each the `ip rip authentication-key` command overrides the previous definition.

Example

The following example shows how to define a password:

```
interface ip 1.1.1.1
  ip rip authentication mode text
  ip rip authentication-key alph$$12
exit
```
54.7  **ip rip default-information originate**

The `ip rip default-information originate` IP Interface generates a metric for a default route in RIP. The `no` format of the command disables the feature.

**Syntax**

```
ip rip default-information originate {disable | metric}
nop ip rip default-information originate
```

**Parameters ranges**

- `disable`—Do not send the default route.

**Default Configuration**

The RIP behavior is specified by the `default-information originate` command.

**Command Mode**

IP interface mode

**User Guidelines**

Use the command to override the RIP behavior specified by the `default-information originate` command on a given IP interface.

**Example**

The following example shows how to enable sending of default route with metric 3:

```
interface ip 1.1.1.1
  ip rip default-information originate 3
exit
```

---

54.8  **ip rip distribute-list in**

The `ip rip distribute-list in` IP configuration mode command enables filtering of routes in incoming RIP Update messages. The `no` format of the command disables the filtering.
**RIP Commands**

**Syntax**

`ip rip distribute-list {access access-list-name} in`

`no ip rip distribute-list in`

**Parameters**

- **access-list-name**—Standard IP access list name, up to 32 characters. The list defines which routes in incoming RIP Update messages are to be accepted and which are to be suppressed.

**Default Configuration**

No filtering

**Command Mode**

IP interface mode

**User Guidelines**

Each network from a received RIP Update message is evaluated by the access list and it is accepted only if it is permitted by the list. See the `ip access-list (IP standard)` command for details.

**Example**

The following example shows how to define input filtering:

```
interface ip 1.1.1.1
  ip rip distribute-list 5 in
exit
```

---

**54.9 ip rip distribute-list out**

The `ip rip distribute-list out` IP configuration mode command enables filtering of routes in outgoing RIP Update messages. The `no` format of the command disables the filtering.

**Syntax**

`ip rip distribute-list {access access-list-name} out`
no ip rip distribute-list out

Parameters

- access-list-name—Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP Update messages are to be sent and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP interface mode

User Guidelines

Each network from the IP Forwarding table is evaluated by the list and it is included in the RIP Update message only if it is permitted by the list. About details see the ip access-list (IP standard) command.

Example

The following example shows how to define outgoing filtering:

```console
Console(config)# interface ip 1.1.1.1
Console(config-ip)# ip rip distribute-list 5 out
```

54.10 ip rip offset

The ip rip offset IP configuration mode command defines a metric added to incoming routes. The no format of the command returns to default.

Syntax

ip rip offset offset

no ip rip offset

Parameters

offset—Specifies the offset to be applied to received routes. Range: 1-15.
**Default Configuration**

offset—1.

**Command Mode**

IP interface mode

**User Guidelines**

**Example**

The following example shows how to set offset to 2:

```
interface ip 1.1.1.1
   ip rip offset 2
exit
```

### 54.11 ip rip passive-interface

The **ip rip passive-interface** IP Interface Configuration mode command disables sending RIP packets on an IP interface. The **no** format of the command re-enables the sending RIP packets.

**Syntax**

- `ip rip passive-interface`
- `no ip rip passive-interface`

**Parameters**

N/A.

**Default Configuration**

RIP messages are sent.

**Command Mode**

IP interface mode
User Guidelines

Use the `ip rip passive-interface` command to stop of RIP messages sending on the giving IP interface. To stop RIP messages being sent on all interfaces, use the `passive-interface` command.

Note. The `no ip rip passive-interface` command does not override the `passive-interface` command.

Example

The following example shows how to stop the sending of RIP messages:

```bash
interface ip 1.1.1.1
    ip rip passive-interface
exit
```

54.12 ip rip shutdown

The `ip rip shutdown` IP Interface configuration mode command changes the RIP interface state from enabled to disabled. The `no` format of the command returns the state to a value of enabled.

Syntax

`ip rip shutdown`

`no ip rip shutdown`

Parameters

N/A

Default Configuration

Enabled

Command Mode

IP Interface mode.

User Guidelines

Use the `ip rip shutdown` CLI command to disable RIP on an IP interface without removing its configuration. The `ip rip shutdown` CLI command may be applied only
to RIP interfaces created by the `network` CLI command. The `ip rip shutdown` CLI command does not remove the RIP interface configuration.

**Example**

The following example shows how to disable RIP on the 1.1.1.1 IP interface:

```plaintext
interface ip 1.1.1.1
  ip rip shutdown
exit
```

---

### 54.13 network

The `network` Router RIP configuration mode command enables RIP on the given IP interfaces. The `no` format of the command disables RIP on the given IP interfaces and removes its interface configuration.

**Syntax**

```plaintext
network ip-address [shutdown]
no network ip-address
```

**Parameters**

- `ip-address` — An IP address of a switch IP interface.
- `shutdown` — RIP is enabled on the interface in the shutdown state.

**Default Configuration**

N/A

**Command Mode**

Router RIP configuration.

**User Guidelines**

RIP can be defined only on manually configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.

Use the `network` CLI command with the `shutdown` keyword to create RIP on an interface if you are going to change the default values of RIP configuration and the use the `no ip rip shutdown` CLI command.
Use the no network CLI command to remove RIP on an IP interface and remove its interface configuration.

Example

Example 1. The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:

```
router rip
    network 1.1.1.1
exit
```

Example 2. The following example enables RIP on 1.1.1.1 in the shutdown state, configures metric and starts RIP:

```
router rip
    network 1.1.1.1 shutdown
exit
interface ip 1.1.1.1
    ip rip offset 2
    no ip rip shutdown
exit
```

54.14 passive-interface (RIP)

To disable sending routing updates on all RIP IP interfaces, use the passive-interface command in router configuration mode. To re-enable the sending of RIP routing updates, use the no form of this command.

Syntax

```
passive-interface

no passive-interface
```

Parameters

N/A
Default Configuration
Routing updates are sent on all OSPF IP interfaces.

Command Mode
Router configuration (config-router)

User Guidelines
After using the passive-interface command, you can then configure individual interfaces where adjacencies are desired using the no ip rip passive-interface command.

Example
The following example sets all IP interfaces as passive and then excludes the IP interface 1.1.1.1:

```
router rip
  passive-interface
  network 1.1.1.1
  network 2.2.2.2
  network 3.3.3.3
exit
interface ip 1.1.1.1
  no ip rip passive-interface
exit
```

54.15 redistribute (RIP)
To redistribute routes from one routing domain into a RIP routing domain, use the redistribute command in the Router RIP configuration mode. To disable redistribution, use the no form of this command.

Syntax

```
redistribute protocol [process-id] [metric {metric-value | transparent}] [match {internal | external 1 | external 2}] [route-map map-tag]
```
no redistribute protocol\[process-id\] [metric \{metric-value | transparent\}] [match \{internal | external 1 | external 2\}] [route-map map-tag]

Parameters

- **protocol**—Source protocol from which routes are being redistributed. It can be one of the following keywords: `connected` or `static`.

- **metric transparent**—Causes RIP to use the source protocol metric for redistributed routes as the RIP metric. Only routes with metric less than 16 are redistributed.

- **metric metric-value**—Specifies the metric assigned to the redistributed routes. The value supersedes the metric value specified using the `default-metric` command.

- If the metric value is set by the route map (by the `set metric` command) then the value will supersede the metric value specified by the `metric-value` argument.

  If the `metric` keyword is not defined, then the metric is specified by the `default-metric` CLI command is assigned to the redistributed routes. If metric value set by the route map is equal or bigger than 16 the route is not redistributed.

Default Configuration

Route redistribution is disabled

Command Mode

Router RIP configuration.

User Guidelines

Routes distributed to the source protocol are never redistributed by it

The `connected` keyword is used to redistribute to RIP routes that correspond to defined IP interfaces on which RIP is not enabled. By default, the RIP Routing Table includes only routes that correspond only to IP interfaces on which it is enabled.

The `static` keyword is used to redistribute to RIP static routes. By default, static routes are not redistributed to RIP.

Removing options that you have configured for the `redistribute` command requires careful use of the `no` form of the `redistribute` command to ensure that you obtain the result that you are expecting.
Example

Example 1. The following example enables redistribution of static routes by RIP with transparent metric:

```
router rip
    redistribute static metric transparent
exit
```

Example 2. The following example enables redistribution of static routes by RIP with transparent metric and then changes the metric to default:

```
router rip
    redistribute static metric transparent
    no redistribute static metric transparent
exit
```

Example 3. The following example enables redistribution of static routes by RIP with default metric and then changes the metric to transparent:

```
router rip
    redistribute static
    redistribute static metric transparent
exit
```

Example 4. The following example enables redistribution of static routes by RIP with transparent metric. The second redistribute command does not affect:

```
router rip
    redistribute static metric transparent
    redistribute static
exit
```
**Example 5.** The following example disables redistribution of static routes by RIP:

```
router rip
  no redistribute static
exit
```

**Example 6.** The following example removes the metric 5 option causing using of a metric defined by the default-metric CLI command:

```
router rip
  no redistribute static metric 1000
exit
```

### 54.16 router rip

The `router rip` Global Configuration mode command specifies the Router RIP mode and enables it if it was disabled. The `no` format of the command disables RIP globally and removes its configuration.

**Syntax**

```
router rip
no router rip
```

**Parameters**

N/A

**Default Configuration**

Disabled
**Command Mode**

Global Configuration mode

**User Guidelines**

RIP supports the following global states:

- disabled
- enabled
- shutdown

If a value of the RIP global state is **disabled** (default value), RIP is not operational and cannot be configured. When the state is set, the RIP configuration is removed. The state may be set by the `no router rip` CLI command from any RIP global state.

If a value of the RIP global state is **shutdown**, RIP is not operational, but can be configured. When the state is set, the RIP configuration is not changed. The state may be set by the `shutdown` CLI command from the **enabled** RIP global state.

If the value of the RIP global state is **enabled**, RIP is operational, and can be configured. The state may be set by the `router rip` CLI command from the **disabled** RIP global state and by the `no shutdown` CLI command from the **shutdown** RIP global state.

**Example**

The following example shows how to enable RIP globally:

```
router rip
```

**54.17 show ip rip database**

The `show ip rip database` Privileged EXEC mode command displays information about RIP Database.

**Syntax**

```
show ip rip database [all | brief | ip-address]
```

**Parameters**

- **all**—Provides the full RIP database information about all RIP interfaces. The option is assumed if the parameter is omitted.
- **brief**—Provides a summary view of the RIP database information
- **ip-address**—Provides the full RIP database information about the given IP Address.

**Command Mode**

Privileged EXEC mode

**Default Configuration**

N/A

**Examples**

**Example 1**—The following example shows the full RIP database information about all RIP interfaces is displayed:

```
Console# show ip rip database
RIP is enabled
RIP Administrative state is UP
Default metric value is 1
Redistributing is enabled from
  Connected:
    Metric is default-metric
    Static:
      Metric is transparent with subnets
  IP Interface: 1.1.1.1
Administration State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
```
Example 2—The following example shows the full RIP database information about a given IP address is displayed:

```
Console# show ip rip database 1.1.1.1
RIP is enabled
```
RIP Administrative state is UP
Default Originate Metric: on passive only
Default metric value is 1
Redistributing is enabled from Connected
  Metric is default-metric
Static:
  Metric is transparent
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12

Example 3—The following example shows the brief RIP database information about all RIP interfaces is displayed:

Console#show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Default metric value is 1
Redistributing is enabled from Connected
  Metric is default-metric
Static
  Metric is transparent
IP Interface    Admin  Offset  Passive Default Auth. IN Filt. OUT Filt.
<table>
<thead>
<tr>
<th>State</th>
<th>Interface Metric</th>
<th>Type</th>
<th>Type</th>
<th>Type</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.100.100.100 enabled</td>
<td>10</td>
<td>No</td>
<td>12</td>
<td>Text</td>
<td>Access</td>
</tr>
<tr>
<td>2.2.2.2 enabled</td>
<td>2</td>
<td>No</td>
<td>MD5</td>
<td>Prefix</td>
<td>Access</td>
</tr>
<tr>
<td>3.3.3.3 enabled</td>
<td>1</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4.4.4 shutdown</td>
<td>1</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example 4**—The following example shows the output when RIP is disabled:

```
Console#show ip rip database
RIP is disabled
```

### 54.18 show ip rip peers

The `show ip rip peers` Privileged EXEC mode command displays information about RIP Peers.

**Syntax**

```
show ip rip peers
```

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**Default Configuration**

N/A

**Example**

```
Console#show ip rip peers
RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1
Address Last Received Received
```
54.19 show ip rip statistics

The show ip rip statistics Privileged EXEC mode command displays RIP Statistics.

Syntax

show ip rip statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Example

Console#show ip rip statistics
RIP is enabled
Static redistributing is enabled with transparent metric
Default redistributing metric is 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received Bad</th>
<th>Received Bad Pakets</th>
<th>Sent Triggered</th>
<th>Sent Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>00:10:17</td>
<td></td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>00:10:01</td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### 54.20 shutdown

The `shutdown` Router RIP configuration mode command sets the RIP global state to `shutdown`. The `no` format of the command sets the RIP global state to `enabled`.

**Syntax**

```
shutdown
no shutdown
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Router RIP configuration.

**User Guidelines**

Use the `shutdown` CLI command to stop RIP globally without removing its configuration.

**Example**

The following example shows how to shutdown RIP globally:

```
router rip
  shutdown

exit
```
Router Resources Commands

55.1 system router resources

Use the system router resources command in Global Configuration mode to configure the system router resources. To return to the default, use the no form of this command.

Syntax

system router resources [ip-entries max-number] [ipv6-entries max-number] no system router resources

Parameters

- ip-entries— The maximum number of IPv4 entries.
- ipv6-entries— The maximum number of IPv6 entries.

Default Configuration

Product specific

Command Mode

Global configuration

User Guidelines

Use the system router resources command to enter new settings for routing entries. After entering the command, the current routing entries configuration will be displayed, and the user will be required to confirm saving the new setting to the startup-configuration and to reboot the system.

When this command is included in a configuration file that is downloaded to the device, if it is downloaded to the running configuration file, the command will be rejected. If it downloaded to the startup configuration file, the device will not be automatically rebooted. The new settings will be used after the device is rebooted manually.

Data Validation:

If the new settings exceed the maximum number of routing entries, the command is rejected and a message is displayed to the user.
If the new settings are lower than the currently in-use routing entries, a confirmation message is displayed to the user (before the save confirmation message).

Use the `no system router resources` command to the default settings.

The following table displays the conversion between logical entities to HW entries:

**Table 4: IPv4**

<table>
<thead>
<tr>
<th>Logical Entity</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Neighbor</td>
<td>1 entry</td>
</tr>
<tr>
<td>IP Address</td>
<td>2 entries</td>
</tr>
<tr>
<td>IP Remote Route</td>
<td>1 entry</td>
</tr>
</tbody>
</table>

**Table 5: IPv6**

<table>
<thead>
<tr>
<th>Logical Entity</th>
<th>IPv6 (PCL TCAM)</th>
<th>IPv6 (Router TCAM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Neighbor</td>
<td>1 entry</td>
<td>4 Entries</td>
</tr>
<tr>
<td>IP Address</td>
<td>2 entries</td>
<td>8 entries</td>
</tr>
<tr>
<td>IP Remote Route</td>
<td>1 entry</td>
<td>4 Entries</td>
</tr>
<tr>
<td>On-Link-Prefix</td>
<td>1 Entry</td>
<td>4 Entries</td>
</tr>
</tbody>
</table>

**Examples**

**Example 1**

The following example defines the supported number of IPv4 and IPv6 routing entries. In the example, the configured router entries are less than the router entries which are currently in use. Using this configurations means that the system will not have enough resources for the running again in the existing network:

```
switchxxxxxx(config)# system router resources ip-routes 128 ipv6-routes 32
```

The maximal number of IPv4 Routing entries and IPv6 Routing Entries is 3072. The number is Non-IP Entries is 3096.

<table>
<thead>
<tr>
<th>In-Use</th>
<th>Reserved (Current)</th>
<th>Reserved (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
IPv4 Entries       232   1024   128
  Number of Routes  20
  Number of Neighbors  12
  Number of Interfaces  100
IPv6 Entries       1024  1024   32
  Number of Routes  20
  Number of Neighbors  12
  Number of Interfaces  100
  Number of On-Link Prefixes  1

Non-IP Entries:
- Unit 1          93%   400
- Unit 2          94%   400
- Unit 5          90%   400

The new configuration of route entries is less than the route entries which are currently in use by the system, do you want to continue (note that setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system)? (Y/N) [N] Y

Example 2

The following example defines the supported number of IPv4 routing entries.

```
switchxxxxxx(config)#system router resources ip-routes 256
```

The maximal number of IPv4 and IPv6 Routing Entries is 3072. The number is Non-IP Entries is 3096.

```
 In-Use   Reserved (Current)  Reserved (New)
--------  -------------------  ------------
IPv4 Entries       232   1024   256
  Number of Routes  20
  Number of Neighbors  12
  Number of Interfaces  100

Non-IP Entries:
```
Setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system, do you want to continue? (Y/N) [N] Y

55.2  show system router resources

Use the show system router resources command in EXEC mode to display the router resources.

**Syntax**

```
show system router resources
```

**Parameters**

This command has no arguments or keywords.

**Command Mode**

EXEC mode

**Example**

**Example 1.** In the following example, the configured router entries are displayed:

```
switchxxxxxx# show system router resources
```

The maximal number of IPv4 and IPv6 Routing Entries is 3072. The number is Non-IP Entries is 3096.

```
In-Use     Reserved
------     --------
IPv4 Entries  232    1024
Number of Routes  20
Number of Neighbors  12
Number of Interfaces  100
```
### Non-IP Entries:

- Unit 1  | 93%  | 400
- Unit 2  | 94%  | 400
- Unit 5  | 90%  | 400
DHCPv6 Commands

56.1 ipv6 dhcp client stateless

Use the `ipv6 dhcp client stateless` command in Interface Configuration mode to enable DHCP for an IPv6 client process and to enable request for stateless configuration through the interface on which the command is run. To disable requests for stateless configuration, use the `no` form of this command.

Syntax

```
ipv6 dhcp client stateless
no ipv6 dhcp client stateless
```

Parameters

This command has no arguments or keywords.

Default Configuration

Information request is disabled on an interface.

Command Mode

Interface configuration

User Guidelines

Enabling this command starts the DHCPv6 client process if this process is not yet running and IPv6 interface is enabled on the interface.

This command enables the DHCPv6 Stateless service on the interface. The service allows to receive the some configuration from a DHCP server passed in the following options:

- Option 23: OPTION_DNS_SERVERS - List of DNS Servers IPv6 Addresses
- Option 24: OPTION_DOMAIN_LIST - Domain Search List
- Option 31: OPTION_SNTP_SERVERS - List of SNTP Servers IPv6 Addresses
- Option 32: OPTION_INFORMATION_REFRESH_TIME - Information Refresh Time Option
- Option 41: OPTION_NEW_POSIX_TIMEZONE - New Timezone Posix String
- Option 59: OPT_BOOTFILE_URL - Configuration Server URL
- Option 60: OPT_BOOTFILE_PARAM, the first parameter - Configuration File Path Name

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

Example

The following example enables the Stateless service:

```
interface vlan 100
  ipv6 dhcp client stateless
exit
```

56.2 clear ipv6 dhcp client

Use the `clear ipv6 dhcp client` command in Privileged EXEC mode to restart DHCP for an IPv6 client on an interface.

Syntax

```
clear ipv6 dhcp client interface-id
```

Parameters

`interface-id`— Interface identifier.

Default Configuration

N/A

Command Mode

Privileged EXEC.
User Guidelines

This command restarts DHCP for an IPv6 client on a specified interface after first releasing and unconfiguring previously-acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Example

The following example restarts the DHCP for IPv6 client on VLAN 100:

```
clear ipv6 dhcp client vlan 100
```

56.3 ipv6 dhcp client information refresh

To configure the refresh time for IPv6 client information refresh time on a specified interface if the DHCPv6 server reply does not include the Information Refresh Time, use the `ipv6 dhcp client information refresh` command in Interface Configuration mode. To return to the default value of the refresh time, use the `no` form of this command.

Syntax

```
ipv6 dhcp client information refresh seconds | infinite
no ipv6 dhcp client information refresh
```

Parameters

- **seconds**— The refresh time, in seconds. The value cannot be less than the minimal acceptable refresh time configured by the `ipv6 dhcp client information refresh` command. The maximum value that can be used is 4,294967,294 seconds (0xFFFFFFFF).

- **infinite**— Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface configuration (config-if).
User Guidelines

The `ipv6 dhcp client information refresh` command specifies the information refresh time. If the server does not send an information refresh time option then a value configured by the command is used.

Use the `infinite` keyword, to delete refresh, if the server does not send an information refresh time option.

Example

The following example configures an upper limit of 2 days:

```
interface vlan 100
   ipv6 dhcp client stateless
   ipv6 dhcp client information refresh 172800
exit
```

56.4 `ipv6 dhcp client information refresh minimum`

To configure the minimum acceptable refresh time on the specified interface, use the `ipv6 dhcp client information refresh minimum` command in Interface Configuration mode. To remove the configured refresh time, use the `no` form of this command.

Syntax

```
ipv6 dhcp client information refresh minimum seconds/infinite
no ipv6 dhcp client information refresh minimum
```

Parameters

- `seconds`— The refresh time, in seconds. The minimum value that can be used is 600 seconds. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFF).
- `infinite`— Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).
**DHCPv6 Commands**

**Command Mode**

Interface configuration (config-if).

**User Guidelines**

The `ipv6 dhcp client information refresh minimum` command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

If you configure the `infinite` keyword client never refreshes the information.

**Example**

The following example configures an upper limit of 2 days:

```plaintext
interface vlan 100
  ipv6 dhcp client stateless
  ipv6 dhcp client information refresh 172800
exit
```

**56.5 ipv6 dhcp duid-en**

Use the `ipv6 dhcp duid-en` command in Global Configuration mode to set the Vendor Based on Enterprise Number DHVPv6 Unique Identified (DUID-EN) format.

To return to the default value, use the `no` form of this command.

**Syntax**

`ipv6 dhcp duid-en enterprise-number identifier`

`no ipv6 dhcp duid-en`
Parameters

- **enterprise-number**—The vendor’s registered Private Enterprise number as maintained by IANA.
- **identifier**—The vendor-defined hex string (up to 64 hex characters). If the number of the character is not even, an ‘0’ is added at the right. Each 2 hex characters can be separated by a period or colon.

Default Configuration

DUID Based on Link-layer Address (DUID-LL) is used. The base MAC Address is used as a Link-layer Address.

Command Mode

Global Configuration.

User Guidelines

By default, the DHCPv6 uses the DUID Based on Link-layer Address (see RFC3315) with the Base MAC Address as a Link-layer Address.

Use this command to change the UDID format to the Vendor Based on Enterprise Number.

Example

**Example 1.** The following sets the DIID-EN format:

```
ipv6 dhcp udid-en 9 0CC084D303000912
```

**Example 2.** The following sets the DIID-EN format using colons as delimiter:

```
ipv6 dhcp udid-en 9 0C:C0:84:D3:03:00:09:12
```

56.6 ipv6 dhcp relay destination (Global)

To specify a globally defined relay destination address to which client messages are forwarded, use the **ipv6 dhcp relay destination** command in global configuration mode. To remove a relay destination address, use the **no** form of this command.
Syntax

ipv6 dhcp relay destination {ipv6-address [interface-id]} | interface-id
no ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id

Parameters

- **ipv6-address**— Relay destination address. There are the following types of relay destination address:
  - Link-local unicast. A user must specify an output interface for this kind of address.
  - Global unicast IPv6 address. An output interface cannot be specified for this kind of address.

This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.

If the argument is not configured then the well know the link-local multicast address All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is defined.

- **interface-id**— Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected. If this argument is omitted then the Routing table is used.

Default Configuration

There is no globally defined relay destination.

Command Mode

Global configuration mode

User Guidelines

The `ipv6 dhcp relay destination` command specifies a destination address to which client messages are forwarded. The address is used by all DHCPv6 relay running in the switch.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per the interface and globally.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays
messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination.

Use the no form of the command with the ipv6-address and interface-id arguments to remove only the given globally defined address with the given output interface.

Use the no form of the command with the ipv6-address argument to remove only the given globally defined address for all output interfaces.

The no form of the command without the arguments removes all the globally defined addresses.

Example

Example 1. The following example sets the relay unicast link-local destination address per VLAN 200:

```
ipv6 dhcp relay destination FE80::1:2 vlan 200
```

Example 2. The following example sets the relay well known multicast link-local destination address per VLAN 200:

```
ipv6 dhcp relay destination vlan 200
```

Example 3. The following example sets the unicast global relay destination address:

```
ipv6 dhcp relay destination 3002::1:2
```

56.7 ipv6 dhcp relay destination (Interface)

To specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface, use the ipv6 dhcp relay destination command in Interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the no form of this command.
Syntax

```
ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id
no ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id
```

Parameters

- **ipv6-address**— Relay destination address. The following types of relay destination addresses exist:
  - Link-local unicast. A user must specify an output interface for this kind of address.
  - Global unicast IPv6 address. An output interface cannot be specified for this kind of address.

  This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.

  If the argument is not configured then the well-known link-local Multicast address All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is defined.

- **interface-id**—Specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Default Configuration

The relay function is disabled, and there is no relay destination on an interface.

Command Mode

Interface configuration (config-if)

User Guidelines

This command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface.

DHCPv6 Relay inserts the Interface-id option if an IPv6 global address is not defined on the interface on which the relay is running. The Interface-id field of the option is the interface name (a value of the ifName field of the ifTable) on which the relay is running.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per the interface and globally.
The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a Unicast address of a server or another relay agent, or it may be a Multicast address. There are two types of relay destination addresses:

- A link-local Unicast or Multicast IPv6 address, for which a user must specify an output interface.
- A global Unicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a Unicast or Multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local Multicast addresses are not acceptable as the relay destination.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface.

Use the no form of the command with arguments to remove a specific address.

Use the no form of the command without arguments to remove all the defined addresses and to disable the relay on the interface.

**Example**

**Example 1.** The following example sets the relay Unicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```plaintext
interface vlan 100

ipv6 dhcp relay destination FE80::1:2 vlan 200

exit
```
**Example 2.** The following example sets the relay well known Multicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```plaintext
interface vlan 100
   ipv6 dhcp relay destination vlan 200
exit
```

**Example 3.** The following example sets the Unicast global relay destination address and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```plaintext
interface vlan 100
   ipv6 dhcp relay destination 3002::1:2
exit
```

**Example 4.** The following example enables the DHCPv6 relay on VLAN 100:

```plaintext
interface vlan 100
   ipv6 dhcp relay destination
exit
```

**Example 5.** The following example disables the DHCPv6 relay on VLAN 100:

```plaintext
interface vlan 100
   no ipv6 dhcp relay destination
exit
```

### 56.8 show ipv6 dhcp

Use the `show ipv6 dhcp` command in User EXEC or Privileged EXEC mode to display the Dynamic DHCP unique identifier (DUID) on a specified device. This information is relevant for DHCPv6 client and DHCPv6 relay.
Syntax
show ipv6 dhcp

Parameters
NA

Command Mode
User EXEC
Privileged EXEC

User Guidelines
This command uses the DUID, based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

Example

Example 1. The following is sample output from this command when the switch’s UDID format is Vendor Based on Enterprise Number:

```
show ipv6 dhcp
The switch’s DHCPv6 unique identifier (DUID) is 0002000000090CC084D303000912
    Format: 2
    Enterprise Number: 9
    Identifier: 0CC084D303000912
```

Example 2. The following is sample output from this command when the switch’s UDID format is the vendor-based on link-layer address:

```
show ipv6 dhcp
The switch’s DHCPv6 unique identifier (DUID) is 000300010024012607AA
    Format: 3
    Hardware type: 1
    MAC Address: 0024.0126.07AA
```
56.9  **show ipv6 dhcp interface**

Use the **show ipv6 dhcp interface** command in User EXEC or Privileged EXEC mode to display DHCP for IPv6 interface information.

**Syntax**

```
show ipv6 dhcp interface [interface-id]
```

**Parameters**

*interface-id*— Interface identifier.

**Command Mode**

User EXEC
Privileged EXEC

**User Guidelines**

If no interfaces are specified in the command, all interfaces on which DHCP for IPv6 (client or server) is enabled are displayed. If an interface is specified in the command, only information about the specified interface is displayed.

**Example**

**Example 1.** The following is sample output from this command when only the Stateless service is enabled:

```
show ipv6 dhcp interface
FastEthernet 1/0/1 is in client mode
  DHCP Operational mode is enabled
  Stateless Service is enabled
  Reconfigure service is enabled
  Information Refresh Minimum Time: 600 seconds
  Information Refresh Time: 86400 seconds
  Received Information Refresh Time: 3600 seconds
  Remain Information Refresh Time: 411 seconds
  DHCP server:
    Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
```
Preference: 20
DNS Servers: 1001::1, 2001::10
DNS Domain Search List: company.com beta.org
SNTP Servers: 2004::1
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Configuration Server: config.company.com
Configuration Path Name: qqq/config/aaa_config.dat
Indirect Image Path Name: qqq/config/aaa_image_name.txt

FastEthernet 1/0/2 is in client mode
DHCP Operational mode is disabled (IPv6 is not enabled)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds

FastEthernet 1/0/3 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds

FastEthernet 1/0/4 is in relay mode
DHCP Operational mode is enabled
Relay source interface: VLAN 101
Relay destinations:
  FE80::250:A2FF:FE8F:A056 via FastEthernet 1/0/10

FastEthernet 1/0/5 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
DHCP server:
  Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
Received Information Refresh Time: 3600 seconds
DNS Servers: 1001::1, 2001::10
DNS Domain Search List: company.com beta.org
SNTP Servers: 2004::1
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Configuration Server: config.company.com
Configuration Path Name: qqq/config/aaa_config.dat
Indirect Image Path Name: qqq/config/aaa_image_name.txt
DHCP Server Commands

57.1 ip dhcp server

Use the `ip dhcp server` Global Configuration mode command to enable the DHCP server features on the device.

Use the `no` form of this command to disable the DHCP server.

Syntax

```
ip dhcp server
no ip dhcp server
```

Default Configuration

The DHCP server is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP server on the device:

```
switchxxxxxx(config)# ip dhcp server
```

57.2 ip dhcp pool host

Use the `ip dhcp pool host` Global Configuration mode command to configure a DHCP static address on a DHCP Server and enter the DHCP Pool Host Configuration mode.

Use the `no` form of this command to remove the address pool.

Syntax

```
ip dhcp pool host name
no ip dhcp pool host name
```
Parameters

name—Specifies the DHCP address pool name. It can be either a symbolic string (such as Engineering) or an integer (such as 8). (Length: 1–32 characters)

Default Configuration

DHCP hosts are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example

The following example configures station as the DHCP address pool:

```
switchxxxxxx(config)# ip dhcp pool host station
switchxxxxxx(config-dhcp)#
```

57.3  ip dhcp pool network

Use the `ip dhcp pool network` Global Configuration mode command to configure a DHCP address pool on a DHCP Server and enter DHCP Pool Configuration mode.

Use the `no` form of this command to remove the address pool.

Syntax

```
ip dhcp pool network name
no ip dhcp pool network name
```

Parameters

name—Specifies the DHCP address pool name. It can be either a symbolic string (such as ‘engineering’) or an integer (such as 8). (Length: 1–32 characters)
Default Configuration

DHCP address pools are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example

The following example configures Pool1 as the DHCP address pool.

```
switchxxxxxx(config)# ip dhcp pool network Pool1
switchxxxxxx(config-dhcp)#
```

57.4 address (DHCP Host)

Use the address DHCP Pool Host Configuration mode command to manually bind an IP address to a DHCP client.

Use the no form of this command to remove the IP address binding to the client.

Syntax

```
address ip-address [mask | prefix-length] [client-identifier unique-identifier | hardware-address mac-address]
```

```
no address
```

Parameters

- **address**—Specifies the client IP address.
- **mask**—Specifies the client network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **unique-identifier**—Specifies the distinct client identification in dotted hexadecimal notation. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b70813.8811.66.

- **hardware-address**—Specifies the MAC address.

**Default Configuration**
No address are bound.

**Command Mode**
DHCP Pool Host Configuration mode

**Example**
The following example manually binds an IP address to a DHCP client.

```
switchxxxxxx(config-dhcp)# address 10.12.1.99 255.255.255.0 01b7.0813.8811.66
```

### 57.5 address (DHCP Network)

Use the `address` DHCP Pool Network Configuration mode command to configure the subnet number and mask for a DHCP address pool on a DHCP server.

Use the `no` form of this command to remove the subnet number and mask.

**Syntax**
```
address {network-number | low low-address high high-address} {mask | prefix-length}
no address
```

**Parameters**
- **network-number**—Specifies the IP address of the DHCP address pool.
- **mask**—Specifies the pool network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **low low-address**—Specifies the first IP address to use in the address range.
- **high high-address**—Specifies the last IP address to use in the address range.

**Default Configuration**

DHCP address pools are not configured.

If the low address is not specified, it defaults to the first IP address in the network.

If the high address is not specified, it defaults to the last IP address in the network.

**Command Mode**

DHCP Pool Network Configuration mode

**Example**

The following example configures the subnet number and mask for a DHCP address pool on a DHCP server.

```
switchxxxxxx(config-dhcp)# address 10.12.1.0 255.255.255.0
```

### 57.6 lease

Use the `lease` DHCP Pool Network Configuration mode command to configure the time duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client.

Use the `no` form of this command to restore the default value.

**Syntax**

```
lease {days [[hours] [minutes]] | infinite}
no lease
```

**Parameters**

- **days**—Specifies the number of days in the lease.
- **hours**—Specifies the number of hours in the lease. A `days` value must be supplied before configuring an `hours` value.
DHCP Server Commands

- **minutes**—Specifies the number of minutes in the lease. A **days** value and an **hours** value must be supplied before configuring a **minutes** value.

- **infinite**—Specifies that the duration of the lease is unlimited.

**Default Configuration**

The default lease duration is 1 day.

**Command Mode**

DHCP Pool Network Configuration mode

**Examples**

The following example shows a 1-day lease.

```
switchxxxxxx(config-dhcp)# lease 1
```

The following example shows a one-hour lease.

```
switchxxxxxx(config-dhcp)# lease 0 1
```

The following example shows a one-minute lease.

```
switchxxxxxx(config-dhcp)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
switchxxxxxx(config-dhcp)# lease infinite
```

### 57.7 **client-name**

Use the **client-name** DHCP Pool Host Configuration mode command to define the name of a DHCP client. The client name should not include the domain name.

Use the **no** form of this command to remove the client name.
Syntax

client-name name
no client-name

Parameters

name—Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the name Mars should not be specified as mars.yahoo.com. (Length: 1–32 characters)

Command Mode

DHCP Pool Host Configuration mode

Default Configuration

No client name is defined.

Example

The following example defines the string client1 as the client name.

```
switchxxxxxx(config-dhcp)# client-name client1
```

57.8  default-router

Use the `default-router` DHCP Pool Configuration mode command to configure the default router for a DHCP client.

Use the `no` form of this command to remove the default router.

Syntax

default-router ip-address
no default-router

Parameters

ip-address—Specifies the IP address of a router.

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration
No default router is defined.

User Guidelines
The router IP address should be on the same subnet as the client subnet.

Example
The following example specifies 10.12.1.99 as the default router IP address.

```
switchxxxxxx(config-dhcp)# default-router 10.12.1.99
```

57.9  **dns-server**

Use the **dns-server** DHCP Pool Configuration mode command to configure the Domain Name System (DNS) IP servers available to a DHCP client.

Use the **no** form of this command to remove the DNS server.

**Syntax**

```
dns-server ip-address
no dns-server
```

**Parameters**

*ip-address*—Specifies a DNS server IP address.

**Command Mode**

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

**Default Configuration**

No DNS server is defined.
User Guidelines

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Example

The following example specifies 10.12.1.99 as the client domain name server IP address.

```
switchxxxxxxx(config-dhcp)# dns-server 10.12.1.99
```

57.10 domain-name

Use the `domain-name` DHCP Pool Configuration mode command to specify the domain name for a DHCP client.

Use the `no` form of this command to remove the domain name.

Syntax

```
domain-name domain
no domain-name
```

Parameters

`domain`—Specifies the DHCP client domain name string. (Length: 1–32 characters)

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration

No domain name is defined.

Example

The following example specifies yahoo.com as the DHCP client domain name string.

```
switchxxxxxxx(config-dhcp)# domain-name yahoo.com
```
57.11 netbios-name-server

Use the `netbios-name-server` DHCP Pool Configuration mode command to configure the NetBIOS Windows Internet Naming Service (WINS) servers that are available to Microsoft DHCP clients.

Use the `no` form of this command to remove the NetBIOS name server.

**Syntax**

```
netbios-name-server ip-address
no netbios-name-server
```

**Parameters**

`ip-address`—Specifies the NetBIOS WINS name server IP address.

**Command Mode**

- DHCP Pool Host Configuration mode
- DHCP Pool Network Configuration mode

**Default Configuration**

No bios server is defined.

**Example**

The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
switchxxxxxx(config-dhcp)# netbios-name-server 10.12.1.90
```

57.12 netbios-node-type

Use the `netbios-node-type` DHCP Pool Configuration mode command to configure the NetBIOS node type for Microsoft DHCP clients.

Use the `no` form of this command to return to default.

**Syntax**

```
netbios-node-type {b-node /p-node /m-node /h-node}
```
no netbios-node-type

Parameters

- **b-node**—Specifies the Broadcast NetBIOS node type.
- **p-node**—Specifies the Peer-to-peer NetBIOS node type.
- **m-node**—Specifies the Mixed NetBIOS node type.
- **h-node**—Specifies the Hybrid NetBIOS node type.

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration

h-node (Hybrid NetBIOS node type).

Example

The following example specifies the client's NetBIOS type as mixed.

```
switchxxxxxx(config-dhcp)# netbios node-type m-node
```

### 57.13 next-server

Use the **next-server** DHCP Pool Configuration mode command to configure the next server (siaddr) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the bootfile.

Use the **no** form of this command to remove the boot server.

Syntax

```
next-server ip-address

no next-server
```

Parameters

- **ip-address**—Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
Default Configuration

If the `next-server` command is not used to configure a boot server list, the DHCP server uses inbound interface helper addresses as boot servers.

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Example

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process.

```
switchxxxxxxx(config-dhcp)# next-server 10.12.1.99
```

57.14 `next-server-name`

Use the `next-server-name` DHCP Pool Configuration mode command to configure the next server name (sname) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the bootfile.

Use the `no` form of this command to remove the boot server name.

Syntax

```
next-server-name name
no next-server-name
```

Parameters

`name`—Specifies the name of the next server in the boot process. (Length: 1–64 characters)

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration

No next server name is defined.
Example
The following example specifies www.bootserver.com as the name of the next server in the boot process of a DHCP client.

```
switchxxxxxx(config-dhcp)# next-server www.bootserver.com
```

57.15 bootfile
Use the bootfile DHCP Pool Configuration mode command to specify the default boot image file name for a DHCP client.

Use the no form of this command to delete the boot image file name.

Syntax
```
bootfile filename
no bootfile
```

Parameters
```
filename—Specifies the file name used as a boot image. (Length: 1–128 characters)
```

Command Mode
DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Example
The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
switchxxxxxx(config-dhcp)# bootfile boot_image_file
```

57.16 time-server
Use the time-server DHCP Pool Configuration mode command to specify the time server for a DHCP client.

Use the no form of this command to remove the time server.
Syntax

time-server ip-address
no time-server

Parameters

ip-address—Specifies the IP address of a time server.

Command Mode

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration

No time server name is defined.

User Guidelines

The time server’s IP address should be on the same subnet as the client subnet.

Example

The following example specifies 10.12.1.99 as the time server IP address.

switchxxxxxxx(config-dhcp)# time-server 10.12.1.99

57.17 option

Use the option command in DHCP pool configuration mode to configure the DHCP server options.

Use the no form of this command to remove the options.

Syntax

option code {boolean {false | true} | integer value | ascii string | hex {string | none} | ip {address | ip-list {ip-address 1 [ip-address2 …]}} [description text]}

no option code
Parameters

- **code**—Specifies the DHCP option code. The supported values are defined in the User Guidelines.

- **boolean {false | true}**—Specifies a boolean value. The values are coded by integer values of one octet: 0 = false and 1 = true.

- **integer value**—Specifies an integer value. The option size depends on the option code.

- **ascii string**—Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to the first 160 characters entered.

- **ip address**—Specifies an IP address.

- **ip-list {ip-address1 [ip-address2 ...]}**—Specifies up to 8 IP addresses.

- **hex string**—Specifies dotted hexadecimal data. The hexadecimal value is truncated to the first 320 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.

- **hex none**—Specifies the zero-length hexadecimal string.

- **description text**—User description

Command Mode

- DHCP Pool Host Configuration mode
- DHCP Pool Network Configuration mode

User Guidelines

The **option** command enables defining any option that cannot be defined by other special CLI commands. A new definition of an option overrides the previous definition of this option.

The **boolean** keyword may be configured for the following options: 19, 20, 27, 29-31, 34, 36, and 39.

The **integer** keyword may be configured for the following options: 2, 13, 22-26, 35, 37-38, 132-134, and 211. The switch checks the value range and builds the value field of the size in accordance with the **option** definition.

The **ascii** keyword may be configured for the following options: 14, 17-18, 40, 64, 130, 209, and 210.
The `ip` keyword may be configured for the following options: 16, 28, 32, 128-129, 131, 135, and 136.

The `ip-list` keyword may be configured for the following options: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150.

The `hex` keyword may be configured for any option in the range 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the syntax of an option defined by this format.

**Examples**

**Example 1.** The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding:

```
switchxxxxxx(config-dhcp)# option 19 boolean true description "IP Forwarding Enable/Disable Option"
```

**Example 2.** The following example configures DHCP option 2, which specifies the offset of the client in seconds from Coordinated Universal Time (UTC):

```
switchxxxxxx(config-dhcp)# option 2 integer 3600
```

**Example 3.** The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
switchxxxxxx(config-dhcp)# option 72 ip-list 172.16.3.252 172.16.3.253
```

### 57.18  `ip dhcp excluded-address`

Use the `ip dhcp excluded-address` Global Configuration mode command to specify IP addresses that a DHCP server should not assign to DHCP clients.

Use the `no` form of this command to remove the excluded IP addresses.

**Syntax**

```
ip dhcp excluded-address low-address [high-address]
no ip dhcp excluded-address low-address [high-address]
```
**Parameters**

- **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.

**Default Configuration**

All IP pool addresses are assignable.

**Command Mode**

Global Configuration mode

**User Guidelines**

The DHCP server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

**Example**

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
switchxxxxxx(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

---

### 57.19 clear ip dhcp binding

The **clear ip dhcp binding** Privileged EXEC mode command deletes the dynamic address binding from the DHCP server database.

**Syntax**

```
clear ip dhcp binding {address|*}
```

**Parameters**

- **address**—Specifies the binding address to delete from the DHCP database.
- *****—Clears all automatic bindings.
DHCP Server Commands

### Command Mode

Privileged EXEC mode

### User Guidelines

Typically, the address supplied denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the `no ip dhcp pool` Global Configuration mode command to delete a manual binding.

### Example

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
switchxxxxxx# clear ip dhcp binding 10.12.1.99
```

57.20 **show ip dhcp**

The `show ip dhcp` EXEC mode command displays the DHCP configuration.

### Syntax

```
show ip dhcp
```

### Command Mode

EXEC mode

### Example

The following example displays the DHCP configuration.

```
switchxxxxxx# show ip dhcp
DHCP server is enabled.
```
57.21 **show ip dhcp excluded-addresses**

The `show ip dhcp excluded-addresses` EXEC mode command displays the excluded addresses.

**Syntax**

```
show ip dhcp excluded-addresses
```

**Command Mode**

EXEC mode

**Example**

The following example displays excluded addresses.

```
switchxxxxxx# show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212-10.1.1.219, 10.1.2.212-10.1.2.219
```

57.22 **show ip dhcp pool host**

The `show ip dhcp pool host` EXEC mode command displays the DHCP pool host configuration.

**Syntax**

```
show ip dhcp pool host [address | name]
```

**Parameters**

- **address**—Specifies the client IP address.
- **name**—Specifies the DHCP pool name. (Length: 1-32 characters)

**Command Mode**

EXEC mode
Example

Example 1. The following example displays the configuration of all DHCP host pools:

```
switchxxxxxx# show ip dhcp pool host
The number of host pools is 1
Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
station     172.16.1.11                    01b7.0813.8811.66
```

Example 2. The following example displays the DHCP pool host configuration of the pool named station:

```
switchxxxxxx# show ip dhcp pool host station
Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
station     172.16.1.11                    01b7.0813.8811.66
Mask: 255.255.0.0
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
```
57.23  show ip dhcp pool network

The show ip dhcp pool network EXEC mode command displays the DHCP network configuration.

Syntax

show ip dhcp pool network [name]

Parameters

name—Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

EXEC mode

Example

Example 1—The following example displays configuration of all DHCP network pools:

switchxxxxxx> show ip dhcp pool network
The number of network pools is 2
Name Address range mask Lease
----------------------------------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m

Example 2—The following example displays configuration of the DHCP network pool marketing:

switchxxxxxx> show ip dhcp pool network marketing
Name Address range mask Lease
----------------------------------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
Statistics:
All-range Available Free Pre-allocated Allocated Expired Declined
----------------------------------------------------
Default router: 10.1.1.1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:

57.24 show ip dhcp binding

Use the show ip dhcp binding EXEC mode command to display the specific address binding or all the address bindings on the DHCP server.

Syntax

show ip dhcp binding [ip-address]

Parameters

ip-address—Specifies the IP address

Command Mode

EXEC mode

Examples

The following examples display the DHCP server binding address parameters.

switchxxxxx> show ip dhcp binding

DHCP server enabled
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.1.11</td>
<td>00a0.9802.32de</td>
<td>Feb 01 1998</td>
<td>dynamic</td>
<td>allocated</td>
</tr>
<tr>
<td>1.16.3.23</td>
<td>02c7.f801.0422</td>
<td>12:00AM</td>
<td>dynamic</td>
<td>expired</td>
</tr>
<tr>
<td>1.16.3.24</td>
<td>02c7.f802.0422</td>
<td></td>
<td>dynamic</td>
<td>declined</td>
</tr>
<tr>
<td>1.16.3.25</td>
<td>02c7.f803.0422</td>
<td></td>
<td>dynamic</td>
<td>pre-allocated</td>
</tr>
<tr>
<td>1.16.3.26</td>
<td>02c7.f804.0422</td>
<td></td>
<td>dynamic</td>
<td>declined</td>
</tr>
</tbody>
</table>

switchxxxxx> show ip dhcp binding 1.16.1.11
DHCP server enabled

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.1.11</td>
<td>00a0.9802.32de</td>
<td>Feb 01 1998</td>
<td>dynamic</td>
<td>allocated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12:00 AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

switchxxxxx> show ip dhcp binding 1.16.3.24

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.3.24</td>
<td>02c7.f802.0422</td>
<td></td>
<td>dynamic</td>
<td>declined</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The host IP address as recorded on the DHCP Server.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>The MAC address or client identifier of the host as recorded on the DHCP Server.</td>
</tr>
</tbody>
</table>
show ip dhcp server statistics

Use the `show ip dhcp server statistics` EXEC command to display DHCP server statistics.

**Syntax**

`show ip dhcp server statistics`

**Command Mode**

EXEC mode

**Example**

The following example displays DHCP server statistics

DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
57.26  show ip dhcp allocated

Use the show ip dhcp allocated EXEC mode command to display the allocated address or all the allocated addresses on the DHCP server.

Syntax

show ip dhcp allocated [ip-address]

Parameters

ip-address — Specifies the IP address

Command Mode

EXEC mode

Example

The following example displays the output of various forms of this command:

```
switchxxxxxx> show ip dhcp allocated
DHCP server enabled
The number of allocated entries is 3

+---------------+----------------+-----------------------------+---------+
| IP address    | Hardware address| Lease expiration            | Type    |
|---------------+----------------+-----------------------------+---------|
| 172.16.1.11   | 00a0.9802.32de  | Feb 01 1998 12:00 AM        | Dynamic |
| 172.16.3.253  | 02c7.f800.0422  | Infinite                    | Automatic|
| 172.16.3.254  | 02c7.f800.0422  | Infinite                    | Static  |

switchxxxxxx> show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2

+---------------+----------------+-----------------------------+---------+
| IP address    | Hardware address| Lease expiration            | Type    |
|---------------+----------------+-----------------------------+---------|
| 172.16.3.253  | 02c7.f800.0422  | Infinite                    | Automatic|
| 172.16.3.254  | 02c7.f800.0422  | Infinite                    | Static  |
```
172.16.1.11 00a0.9802.32de  Feb 01 1998 12:00 AM  Dynamic

switchxxxxxx> show ip dhcp allocated 172.16.3.254
DHCP server enabled
The number of allocated entries is 2

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
<th>Lease expiration</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.3.254</td>
<td>02c7.f800.0422</td>
<td>Infinite</td>
<td>Static</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The host IP address as recorded on the DHCP Server.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>The MAC address or client identifier of the host as recorded on the DHCP Server.</td>
</tr>
<tr>
<td>Lease expiration</td>
<td>The lease expiration date of the host IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>The manner in which the IP address was assigned to the host.</td>
</tr>
</tbody>
</table>

**show ip dhcp declined**

Use the `show ip dhcp declined` EXEC command to display the specific declined address or all of the declined addresses on the DHCP server.

**show ip dhcp declined Field Descriptions**

**Syntax**

`show ip dhcp declined [ip-address]`

**Parameters**

- `ip-address`—Specifies the IP address.
Example

The following example displays the output of various forms of this command:

switchxxxxxx> show ip dhcp declined
DHCP server enabled
The number of declined entries is 2
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

switchxxxxxx> show ip dhcp declined 172.16.1.11
DHCP server enabled
The number of declined entries is 2
IP address   Hardware address
172.16.1.11   00a0.9802.32de

57.28 show ip dhcp expired

Use the show ip dhcp expired EXEC command to display the specific expired address or all of the expired addresses on the DHCP server.

Syntax

show ip dhcp expired [ip-address]

Parameters

ip-address—Specifies the IP.

Command Mode

EXEC mode

Example

switchxxxxxx> show ip dhcp expired
DHCP server enabled
The number of expired entries is 1
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

switchxxxxxx> show ip dhcp expired 172.16.1.11
DHCP server enabled
The number of expired entries is 1
IP address   Hardware address
172.16.1.13 00a0.9802.32de

57.29  show ip dhcp pre-allocated

Use the show ip dhcp pre-allocated EXEC command to display the specific
pre-allocated address or all the pre-allocated addresses on the DHCP server.

Syntax
show ip dhcp pre-allocated [ip-address]

Parameters
ip-address—Specifies the IP.

Command Mode
EXEC mode

Examples

switchxxxxxx> show ip dhcp pre-allocated
DHCP server enabled
The number of pre-allocated entries is 1
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

switchxxxxxx> show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled

The number of pre-allocated entries is 1

IP address       Hardware address
172.16.1.15      00a0.9802.32de
58.1 show udld

To display the administrative and operational Unidirectional Link Detection Protocol (UDLD) status, use the show udld command in Privileged EXEC mode.

Syntax

show udld [interface-id] [neighbors]

Parameters

- interface-id—Interface identifier of an Ethernet port.
- neighbors—Displays neighbor information only.

Command Mode

Privileged EXEC

User Guidelines

If you do not enter an interface ID value, the administrative and operational UDLD status for all interfaces on which UDLD is enabled are displayed.

Example

Example 1—This example shows how to display the UDLD state for all interfaces. Most of the fields shown in the display are self-explanatory. Those that are not self-explanatory are defined below.

```plaintext
show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface gi1/1/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
```
Neighbor MAC: 00:00:01:22:33:dd
Neighbor Device name: switch A
Neighbor Port ID: gi1/2/1
Neighbor Message Time: 20 sec
Neighbor Current State: Bidirectional
Neighbor Expiration Time: 7 sec
Neighbor Device ID: 1234544893
Neighbor MAC: 00:00:01:22:33:ff
Neighbor Device name: switch A
Neighbor Port ID: gi1/2/1
Neighbor Message Time: 15 sec
Neighbor Current State: Undetermined
Neighbor Expiration Time: 17 sec

Interface gi1/1/2
Port UDLD mode: normal (default)
Port Current state: Undetermined
Number of detected neighbors: 1
Neighbor Device ID: 1234567753
Neighbor MAC: 00:00:01:22:33:fe
Neighbor Device name: switch A
Neighbor Port ID: gi1/2/1
Neighbor Message Time: 15 sec
Neighbor Current State: Undetermined
Neighbor Expiration Time: 11 sec

Interface gi1/1/3
Port UDLD mode: disabled
Interface gi1/1/4
Port UDLD mode: normal (default)
Port Current state: shutdown
Interface gi1/1/5
Port UDLD mode: normal (default)
Port Current state: detection
Interface gi1/1/6
Port UDLD mode: normal (default)
Port Current state: Undetermined

Field Descriptions:

- **Global UDLD mode**—The global UDLD mode (normal or aggressive) configured by the `udld` command.
- **Message Time**—The message time configured by the `udld message time` command.

- **Port UDLD mode**—The interface UDLD mode (normal or aggressive).

- **Port Current state**—The UDLD operational state: interface UDLD mode (normal or aggressive).
  - **Disabled**—UDLD is disabled on the port by the `udld port disable` command.
  - **Shutdown**—UDLD is enabled on the port and the port operational state is DOWN.
  - **Detection**—UDLD is detecting the link state.
  - **Bidirectional**—The link is bidirectional.
  - **Undetermined**—The link state is undetermined - no UDLD message has been received on the port.

- **Neighbor Device ID**—The device ID of the neighbor.

- **Neighbor MAC**—The MAC address of the neighbor.

- **Neighbor Device name**—The Device name of the neighbor.

- **Neighbor Port ID**—The device port ID of the neighbor on which the recent UDLD message was sent.

- **Neighbor Message Time**—The message time of the neighbor.

- **Neighbor Current State**—The current state of the neighbor:
  - **Bidirectional**—The UDLD messages received from the neighbor contain the Device ID and Port ID of the switch in the Echo TLV.
  - **Undetermined**—The UDLD messages received from the neighbor do not contain the Device ID and Port ID of the switch in the Echo TLV.

- **Neighbor Expiration Time**—Left time in seconds until the current neighbor state expires.

---

**Example 2**—This example shows how to display the UDLD state for one given interface:

```
show udld gi1/1/1

Global UDLD mode: normal
```
Example 3—This example shows how to display neighbor information only:

```
show udld neighbors
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Device ID</th>
<th>Port-ID</th>
<th>Device Name</th>
<th>Message Time (sec)</th>
<th>Neighbor State</th>
<th>Neighbor Expiration Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/0/1</td>
<td>1234567893</td>
<td>gi1/0/1</td>
<td>SAL0734K5R2</td>
<td>15</td>
<td>Bidirectional</td>
<td>11</td>
</tr>
<tr>
<td>gi1/0/2</td>
<td>3456750193</td>
<td>gi1/0/2</td>
<td>SAL0734K5R3</td>
<td>20</td>
<td>Undetermined</td>
<td>5</td>
</tr>
</tbody>
</table>

Example 4—This example shows how to display neighbor information only for a single interface:

```
show udld gi1/0/1 neighbors
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Device ID</th>
<th>Port-ID</th>
<th>Device Name</th>
<th>Message Time (sec)</th>
<th>Neighbor State</th>
<th>Neighbor Expiration Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1/0/1</td>
<td>1234567893</td>
<td>gi1/0/1</td>
<td>SAL0734K5R2</td>
<td>15</td>
<td>Bidirectional</td>
<td>11</td>
</tr>
<tr>
<td>gi1/0/2</td>
<td>3456750193</td>
<td>gi1/0/2</td>
<td>SAL0734K5R3</td>
<td>20</td>
<td>Undetermined</td>
<td>5</td>
</tr>
</tbody>
</table>
58.2 udld

Use the udld command in Global Configuration mode to globally enable the UniDirectional Link Detection (UDLD) protocol. To disable UDLD, use the no form of this command.

Syntax

```
udld aggressive | normal
no udld
```

Parameters

- `aggressive`—Enables UDLD in aggressive mode by default on all fiber interfaces.
- `normal`—Enables UDLD in normal mode by default on all fiber interfaces.

Default Configuration

UDLD is disabled on all fiber interfaces.

Command Mode

Global configuration, Interface Configuration

User Guidelines

This command affects fiber interfaces only. Use the udld port command in Interface Configuration mode to enable UDLD on other interface types.

Use the no form of this command to disable UDLD on all fiber ports.

The device supports the UDLD protocol specified by RFC 5171.

UDLD supports two modes of operation: normal and aggressive. In the aggressive mode the device shuts down a port if it cannot explicitly detect that the link is bidirectional. In the normal mode the device shuts down an interface if it explicitly detect that the link is unidirectional. A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.
You can use the following commands to reset an interface shut down by UDLD:

- The `errdisable recovery reset` command with the `interface interface-id` parameter to reset a given interface.
- The `errdisable recovery reset` command with the `udld` parameter to reset all interfaces shut down by UDLD.
- The `errdisable recovery reset` with the `udld` parameter to automatically recover from the UDLD error-disabled state.

**Example**
This example shows how to enable UDLD on all fiber interfaces:

```
udld normal
```

### 58.3 `udld message time`

Use the `udld message time` command in Global Configuration mode to configure a global value of the interval between two sent probe messages. To return to the default value, use the `no` form of this command.

**Syntax**

```
udld message time seconds
no udld message time
```

**Parameters**

- `seconds`—Interval between two sent probe messages. The valid values are from 1 to 90 seconds.

**Default Configuration**

15 seconds.

**Command Mode**

Global Configuration

**User Guidelines**

Use this command to change the default value of the message interval - the interval between two sequential sent probe messages.
Example
This example shows how to set globally the interval to 40sec:

```
udld message time 40
```

58.4 `udld port`
To enable the UDLD protocol on an Ethernet port, use the `udld port` command in Interface Configuration mode. To return to the default, use the `no` form of this command.

Syntax
```
udld port [aggressive | normal | disable]
```

Parameters
- `aggressive`—Enables UDLD in aggressive mode on this interface.
- `normal`—Enables UDLD in normal mode on this interface. The normal keyword is applied if no keyword is specified.
- `disable`—Disable UDLD on this interface.

Default Configuration
The defaults are as follows:
- Fiber interfaces are in the state of the global `udld` (Disable, Normal or Aggressive).
- Non-fiber interfaces are in the Disable state.

Command Mode
Interface configuration (Ethernet port)

User Guidelines
Use this command on fiber ports to override the setting of the global `udld` command.
If the port changes from fiber to non-fiber or vice versa, all configurations are maintained because the platform software detects a change of module or a Gigabit Interface Converter (GBIC) change.

**Examples**

**Example 1**—This example shows how to enable UDLD in the normal mode on an Ethernet port regardless of the current global `udld` setting:

```
interface gi1/1/1
  udld port normal
exit
```

**Example 2**—This example shows how to return to the default configuration:

```
interface gi1/1/1
  no udld port
exit
```

**Example 3**—This example shows how to disable UDLD on an Ethernet port regardless of the current global `udld` setting:

```
interface gi1/1/1
  udld port disable
exit
```
IPv6 First Hop Security

Policies

Policies contain the rules of verification that will be performed on input packets. They can be attached to VLANs and/or interface (ports or port channels).

The final set of rules that is applied to an input packet on an interface is built in the following way:

1. The rules configured in policies attached to the interface on the VLAN on which the packet arrived are added to the set.

9. The rules configured in the policy attached to the VLAN are added to the set if they have not been added at the port level.

10. The global rules are added to the set if they have not been added at the VLAN or port level.

Rules defined at the port level override the rules set at the VLAN level. Rules defined at the VLAN level override the globally-configured rules. The globally-configured rules override the system defaults.

You can only attach 1 policy (for a specific sub-feature) to a VLAN.

You can attach multiple policies (for a specific sub-feature) to an interface if they specify different VLANs.

A Sub-Feature policy does not take effect until:

- IPv6 First Hop Security is enabled on the VLAN
- The sub-feature is enabled on the VLAN
- The policy is attached to the interface (VLAN, port or LAG).

Default Policies

Empty default polices exist for each sub-feature and are by default attached to all VLANs and interfaces. The default policies are named: "vlan_default" and "port_default".

Rules can be added to these default policies. You do not have to manually attach default policies to interfaces. They are attached by default.
When a user-defined policy is attached to an interface, the default policy for that interface is detached. If the user-defined policy is detached from the interface, the default policy is reattached.

Default policies can never be deleted. You can only delete the user-added configuration.

Lists of Commands

59.1 clear ipv6 first hop security counters

To clear IPv6 First Hop Security interface counters, use the `clear ipv6 first hop security counters` command in privileged EXEC mode.

Syntax

clear ipv6 first hop security counters [interface interface-id]

Parameters

- `interface interface-id`—Clear IPv6 First Hop Security counters for the specified Ethernet port or port channel.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command clears interface counters about packets handled by IPv6 First Hop Security.

Use the `interface` keyword to clear all counters for the specific interface.

Use the command without keyword to clear all counters.

Example

The following example clears IPv6 First Hop Security counters on interface `gi1/1/12`

```
switchxxxxxx#clear ipv6 first hop security counters interface gi1/1/12
```
59.2 clear ipv6 neighbor binding table

To remove dynamic entries from the Neighbor Binding table, use the clear ipv6 neighbor binding table command in Privilege EXEC configuration mode.

Syntax

clear ipv6 neighbor binding table [vlan vlan-id] [interface interface-id] [ipv6 ipv6-address] [mac mac-address]

Parameters

- **vlan vlan-id**—Clear the dynamic entries that match the specified VLAN.
- **interface interface-id**—Clear the dynamic entries that match the specified interface (Ethernet port or port channel).
- **ipv6 ipv6-address**—Clear the dynamic entries that match the specified IPv6 address.
- **mac mac-address**—Clear the dynamic entries that match the specified MAC address.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command deletes the dynamic entries of the Neighbor Binding table.

This command deletes the dynamic entries of the Neighbor Binding table. The dynamic entries to be deleted can be specified by VLAN, interface, IPv6 address, or MAC address.

If no keywords or arguments are entered, all dynamic entries are deleted.

All keyword and argument combinations are allowed.

Example

The following example clears all dynamic entries that exist on vlan 100 & interface gi1/1/1:

```
switchxxxxxx#clear ipv6 neighbor binding table vlan 100 interface gi1/1/1
```
59.3 **device-role (IPv6 DHCP Guard)**

To specify the role of the device attached to the port within an IPv6 DHCP Guard policy, use the `device-role` command in IPv6 DHCPv6 Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
device-role {client | server}
```

```
no device-role
```

**Parameters**

- `client`—Sets the role of the device to DHCPv6 client.
- `server`—Sets the role of the device to DHCPv6 server.

**Default Configuration**

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: client.

**Command Mode**

DHCP Guard Policy Configuration (config-dhcp-guard)

**User Guidelines**

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

IPv6 DHCP Guard discards the following DHCPv6 messages sent by DHCPv6 servers/relays and received on interfaces configured as client:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY
Example

The following example defines an IPv6 DHCP Guard policy named policy 1 and configures the port role as the server:

```
ipv6 dhcp guard policy policy1
  device-role server
exit
```

59.4 device-role (Neighbor Binding)

To specify the role of the device attached to the port within an IPv6 Neighbor Binding policy, use the `device-role` command within an IPv6 Neighbor Binding Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

device-role {perimeter | internal}

no device-role

Parameters

- `perimeter`—Specifies that the port is connected to devices not supporting IPv6 First Hop Security.
- `internal`—Specifies that the port is connected to devices supporting IPv6 First Hop Security.

Default Configuration

Policy attached to port or port channel: Value configured in the policy attached to the VLAN.

Policy attached to VLAN: Perimeter.

Command Mode

Neighbor Binding Policy Configuration (config-nbr-binding)
User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

NB Integrity supports the perimetrečal model (see RFC 6620).

This model specifies two types of ports:

- **Perimeter Port**—Specifies ports connected to devices not supporting NB Integrity. NB Integrity establishes binding for neighbors connected to these ports. The Source Guard does not function on these ports.

- **Internal Port**—The second type specifies ports connected to devices supporting IPv6 First Hop Security. NB Integrity does not establish binding for neighbors connected to these ports, but it does propagate the bindings established on perimeter ports.

Dynamic IPv6 addresses bound to port are deleted when its role is changed from perimetrical to internal. The static IPv6 addresses are kept.

Example

The following example defines a Neighbor Binding policy named policy 1 and configures the port role as an internal port:

```
ipv6 neighbor binding policy policy1
device-role internal
exit
```

59.5 device-role (ND Inspection Policy)

To specify the role of the device attached to the port within an IPv6 ND Inspection policy, use the **device-role** command in ND Inspection Policy Configuration mode. To disable this function, use the **no** form of this command.

**Syntax**

```
device-role {host | router}
no device-role
```
Parameters
- host—Sets the role of the device to host.
- router—Sets the role of the device to router.

Default Configuration
Policy attached to port or port channel: the value configured in the policy attached to the VLAN.
Policy attached to VLAN: host.

Command Mode
ND inspection Policy Configuration (config-nd-inspection)

User Guidelines
If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

ND Inspection performs egress filtering of NDP messages depending on a port role. The following table specifies the filtering rules.

<table>
<thead>
<tr>
<th></th>
<th>Host</th>
<th>Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA</td>
<td>Permit</td>
<td>Permit</td>
</tr>
<tr>
<td>RS</td>
<td>Deny</td>
<td>Permit</td>
</tr>
<tr>
<td>CPA</td>
<td>Permit</td>
<td>Permit</td>
</tr>
<tr>
<td>CPS</td>
<td>Deny</td>
<td>Permit</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Permit</td>
<td>Permit</td>
</tr>
</tbody>
</table>

Example
The following example defines an ND Inspection policy named policy 1 and configures the port role as router:

```
ipv6 nd inspection policy policy1
  device-role router
exit
```
59.6 device-role (RA Guard Policy)

To specify the role of the device attached to the port within an IPv6 RA Guard policy, use the `device-role` command in RA Guard Policy Configuration mode. To returned to the default, use the `no` form of this command.

Syntax

```
device-role {host | router}
no device-role
```

Parameters

- `host`—Sets the role of the device to host.
- `router`—Sets the role of the device to router.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: host.

Command Mode

RA Guard Policy Configuration (config-ra-guard)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

RA Guard discards input RA, CPA, and ICMPv6 Redirect messages received on interfaces configured as host.

Example

The following example defines an RA Guard policy named policy1 and configures the port role as `router`:

```
ipv6 nd raguard policy policy1
   device-role router
exit
```
59.7 drop-unsecure

To enable dropping messages with no or invalid options or an invalid signature within an IPv6 ND Inspection policy, use the `drop-unsecure` command in ND Inspection Policy Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```plaintext
drop-unsecure [enable | disable]

no drop-unsecure
```

**Parameters**

- `enable`—Enables dropping messages with no or invalid options or an invalid signature. If no keyword is configured the `enable` keyword is applied by default.
- `disable`—Disables dropping messages with no or invalid options or an invalid signature.

**Default Configuration**

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

**Command Mode**

ND inspection Policy Configuration (config-nd-inspection)

**User Guidelines**

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

**Example**

The following example defines an ND Inspection policy named `policy1`, places the switch in ND Inspection Policy Configuration mode, and enables the switch to drop messages with no or invalid options or an invalid signature:

```plaintext
ipv6 nd inspection policy policy1
```
59.8 hop-limit

To enable the verification of the advertised Cur Hop Limit value in RA messages within an IPv6 RA Guard policy, use the hop-limit command in RA Guard Policy Configuration mode. To return to the default, use the no form of this command.

Syntax

hop-limit {maximum {value | disable}} [minimum {value | disable}]
no hop-limit [maximum] [minimum]

Parameters

- **maximum value**—Verifies that the hop-count limit is less than or equal to the value argument. Range 1-255. The value of the high boundary must be equal or greater than the value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of the hop-count limit.
- **minimum value**—Verifies that the hop-count limit is greater than or equal to the value argument. Range 1-255.
- **minimum disable**—Disables verification of the lower boundary of the hop-count limit.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration (config-ra-guard)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.
Use the `disable` keyword to disable verification regardless of the global or VLAN configuration.

**Examples**

**Example 1**—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Cur Hop Limit value of 5:

```
ipv6 nd raguard policy policy1
    hop-limit minimum 5
exit
```

**Example 2**—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables validation of the Cur Hop Limit high boundary:

```
ipv6 nd raguard policy policy1
    hop-limit maximum disable
exit
```

### 59.9  ipv6 dhcp guard

To enable the DHCPv6 guard feature on a VLAN, use the `ipv6 dhcp guard` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 dhcp guard
no ipv6 dhcp guard
```

**Parameters**

N/A

**Default Configuration**

DHCPv6 Guard on a VLAN is disabled.
Command Mode
Interface Configuration mode (VLAN)

User Guidelines
DHCPv6 Guard blocks messages sent by DHCPv6 servers/relays to clients received on interfaces that are not configured as a DHCPv6 server. Client messages or messages sent by relay agents from clients to servers are not blocked. See the `device-role (IPv6 DHCP Guard)` command for details.

DHCPv6 Guard validates received DHCPv6 messages based on a DHCPv6 Guard policy attached to the source interface.

Examples
Example 1—The following example enables DHCPv6 Guard on VLAN 100:

```
interface vlan 100
  ipv6 dhcp guard
exit
```

Example 2—The following example enables DHCPv6 Guard on VLANs 100-107:

```
interface range vlan 100-107
  ipv6 dhcp guard
exit
```

59.10 ipv6 dhcp guard attach-policy (port mode)
To attach a DHCPv6 Guard policy to a specific interface, use the `ipv6 dhcp guard attach-policy` command in Interface Configuration mode. To return to the default, use the `no` form of this command.

Syntax
```
ipv6 dhcp guard attach-policy policy-name [vlan vlan-list]
no ipv6 dhcp guard attach-policy [policy-name]
```
Parameters

- **policy-name**—The DHCPv6 Guard policy name (up to 32 characters).
- **vlan vlan-list**—Specifies that the DHCPv6 Guard policy is to be attached to the VLAN(s) in `vlan-list`. If the `vlan` keyword is not configured, the policy is applied to all VLANs on the device on which DHCPv6 Guard is enabled.

Default Configuration

The DHCPv6 Guard default policy is applied.

Command Mode

Interface Configuration (Ethernet port or port channel).

User Guidelines

Use this command to attach a DHCPv6 Guard policy to an interface.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Multiple policies with the `vlan` keyword can be attached to the same interface if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

a. The rules configured in the policy attached to the interface on the VLAN on which the packet arrived are added to the set.

b. The rules configured in the policy attached to the VLAN are added to the set if they have not been added.

c. The global rules are added to the set if they have not been added.

Use `no ipv6 dhcp guard attach-policy` to detach all user-defined DHCP Guard policies attached to the interface.

Use `no ipv6 dhcp guard attach-policy policy-name` to detach the specific `policy-name` from a port.
Examples

Example 1—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/1/1 interface and the default policy port_default is detached:

```
interface gi1/1/1
  ipv6 dhcp guard attach-policy policy1
exit
```

Example 2—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/1/1 interface and applied to VLANs 1-10 and 12-20:

```
interface gi1/1/1
  ipv6 dhcp guard attach-policy policy1 vlan 1-10,12-20
exit
```

Example 3—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/1/1 interface and applied to VLANs 1-10 and the DHCPv6 Guard policy policy2 is attached to the gi1/1/1 interface and applied to VLANs 12-20:

```
interface gi1/1/1
  ipv6 dhcp guard attach-policy policy1 vlan 1-10
  ipv6 dhcp guard attach-policy policy2 vlan 12-20
exit
```

Example 4—In the following example DHCPv6 Guard detaches policy1 from the gi1/1/1 interface:

```
interface gi1/1/1
  no ipv6 dhcp guard attach-policy policy1
exit
```
59.11 ipv6 dhcp guard attach-policy (VLAN mode)

To attach a DHCPv6 Guard policy to a specified VLAN, use the `ipv6 dhcp guard attach-policy` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 dhcp guard attach-policy policy-name
no ipv6 dhcp guard attach-policy
```

**Parameters**

`policy-name`—The DHCPv6 Guard policy name (up to 32 characters).

**Default Configuration**

The DHCPv6 Guard default policy is applied.

**Command Mode**

Interface Configuration mode (VLAN)

**User Guidelines**

Use this command to attach a DHCPv6 Guard policy to a VLAN.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Use the `no` form of the command to detach the current policy and to re-attach the default policy. The `no` form of the command has no effect if the default policy was attached.

**Example**

In the following example, the DHCPv6 Guard policy `policy1` is attached to VLAN 100:

```
interface vlan 100

ipv6 dhcp guard attach-policy policy1

exit
```
59.12 ipv6 dhcp guard policy

To define a DHCP Guard policy and place the switch in DHCPv6 Guard Policy Configuration mode, use the `ipv6 dhcp guard policy` command in Global Configuration mode. To remove the DHCPv6 guard policy, use the `no` form of this command.

Syntax

```
ipv6 dhcp guard policy policy-name
no ipv6 dhcp guard policy policy-name
```

Parameters

`policy-name`—The DHCPv6 Guard policy name (up to 32 characters).

Default Configuration

No DHCPv6 Guard policy are configured

Command Mode

Global Configuration

User Guidelines

This command defines the DHCPv6 Guard policy name, and places the router in DHCPv6 Guard Policy Configuration mode.

The following commands can be configured in IPv6 DHCP Guard Policy Configuration mode:

- `device-role (IPv6 DHCP Guard)`
- `match server address`
- `match reply`
- `preference`

Each policy of the same type (for example, DHCPv6 Guard policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports two predefined, default DHCPv6 Guard policies named: "vlan_default" and "port_default":

```
ipv6 dhcp guard policy vlan_default
exit
```
ipv6 dhcp guard policy port_default
exit

The default policies are empty and cannot be removed, but can be changed. The
no ipv6 dhcp guard policy does not remove the default policies, it only removes
the policy configuration defined by the user.

The default policies cannot be attached by the ipv6 dhcp guard attach-policy
command. The vlan_default policy is attached by default to a VLAN, if no other
policy is attached to the VLAN. The port_default policy is attached by default to a
port, if no other policy is attached to the port.

You can define a policy using the ipv6 dhcp guard policy command multiple times.

Before an attached policy is removed, a request for confirmation is presented to
the user, as shown in Example 3 below.

Examples

Example 1—The following example defines a DHCPv6 Guard policy named
policy1, places the router in DHCPv6 Guard Policy Configuration mode, configures
the port to drop unsecure messages and sets the device role as router:

```
switchxxxxxx(config)#ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)#match server address list1
switchxxxxxx(config-dhcp-guard)#device-role server
switchxxxxxx(config-dhcp-guard)#exit
```

Example 2—The following example defines a DHCPv6 Guard named policy1 by
multiple steps:

```
switchxxxxxx(config)#config
switchxxxxxx(config)#ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)#match server address list1
switchxxxxxx(config-dhcp-guard)#device-role server
switchxxxxxx(config-dhcp-guard)#exit
```

Example 3—The following example removes an attached DHCPv6 Guard policy:

```
switchxxxxxx#config
switchxxxxxx(config)#no ipv6 dhcp guard policy policy1
```

Policy policy1 is applied on the following interfaces:

```
gi1/1/1, gi1/1/2
```

The policy1 will be detached and removed, are you sure [Y/N] Y

### 59.13 ipv6 dhcp guard preference

To globally enable verification of the preference in messages sent by DHCPv6 servers, use the `ipv6 dhcp guard preference` command in Global Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 dhcp guard preference {[maximum value] [minimum value]}
no ipv6 dhcp guard preference [maximum] [minimum]
```

**Parameters**

- **maximum value**—Advertised preference value is lower than or equal to the value argument. Range 0-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum value**—Advertised preference value is greater than or equal to the value argument. Range 0-255.

**Default Configuration**

Verification is not enabled.

**Command Mode**

Global configuration
User Guidelines

This command enables verification that the preference value in messages sent by DHCPv6 servers messages (see RFC3315) is greater than or less than the value argument.

Note. When DHCPv6 Guard receives a RELAY-REPL message, it takes it from the encapsulated message.

Configuring the minimum value keyword and argument specifies the minimum allowed value. The received DHCPv6 reply message with a preference value less than a value specified by the value argument is dropped.

Configuring the maximum value keyword and argument specifies the maximum allowed value. The received DHCPv6 reply message with a preference value greater than the value specified by the value argument is dropped.

Use no ipv6 dhcp guard preference to disable verification of the advertised preference value in DHCPv6 reply messages.

Use no ipv6 dhcp guard preference maximum to disable verification of the maximum boundary of the value of the advertised preference value in DHCPv6 messages.

Use the no ipv6 dhcp guard preference minimum command to disable verification of the minimum boundary of the value of the advertised preference value in DHCPv6 messages.

Examples

Example 1—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using two commands:

```
ipv6 dhcp guard preference minimum 10
ipv6 dhcp guard preference maximum 102
```

Example 2—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using a single command:

```
ipv6 dhcp guard preference minimum 10 maximum 102
```
59.14 ipv6 first hop security

To globally enable IPv6 First Hop Security on a VLAN, use the `ipv6 first hop security` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

ipv6 first hop security

no ipv6 first hop security

**Parameters**

N/A

**Default Configuration**

IPv6 First Hop Security on a VLAN is disabled.

**Command Mode**

Interface Configuration mode (VLAN)

**User Guidelines**

Use the `ipv6 first hop security` command to enable IPv6 First Hop Security on a VLAN.

**Examples**

**Example 1**—The following example enables IPv6 First Hop Security on VLAN 100:

```plaintext
interface vlan 100
    ipv6 first hop security
exit
```

**Example 2**—The following example enables IPv6 First Hop Security on VLANs 100-107:

```plaintext
interface range vlan 100-107
```
ipv6 first hop security

exit

59.15 ipv6 first hop security attach-policy (port mode)

To attach an IPv6 First Hop Security policy to a specific interface, use the **ipv6 first hop security attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

**Syntax**

```markdown
ipv6 first hop security attach-policy policy-name [vlan vlan-list]

no ipv6 first hop security attach-policy [policy-name]
```

**Parameters**

- **policy-name**—The IPv6 First Hop Security policy name (up to 32 characters).
- **vlan vlan-list**—Specifies that the IPv6 First Hop Security policy is to be attached to the VLAN(s) in **vlan-list**. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which IPv6 First Hop Security is enabled.

**Default Configuration**

The IPv6 First Hop Security default policy is applied.

**Command Mode**

Interface Configuration mode (Ethernet port or port channel).

**User Guidelines**

Use this command to attach an IPv6 First Hop Security policy to an interface.

Each succeeding usage of this command overrides the previous usage of the command with the same policy.

If the policy specified by the **policy-name** argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same interface if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:
a. The rules configured in the policy attached to the interface on the VLAN on which the packet arrived, are added to the set.

b. The rules configured in the policy attached to the VLAN are added to the set if they have not been added.

c. The global rules are added to the set if they have not been added.

Use the `no ipv6 first hop security attach-policy` command to detach all user-defined policies attached to the interface. The default policy is reattached.

Use the `no ipv6 first hop security attach-policy policy-name` command to detach the `policy-name` policy from the port.

Examples

Example 1—In the following example, the IPv6 First Hop Security policy `policy1` is attached to the `gi1/1/1` interface:

```
interface gi1/1/1
  ipv6 first hop security attach-policy policy1
exit
```

Example 2—in the following example, the IPv6 First Hop Security policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and 12-20:

```
interface gi1/1/1
  ipv6 first hop security attach-policy policy1 vlan 1-10,12-20
exit
```

Example 3—in the following example, the IPv6 First Hop Security policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and the IPv6 First Hop Security policy `policy2` is attached to the `gi1/1/1` interface and applied to VLANs 12-20:

```
interface gi1/1/1
  ipv6 first hop security attach-policy policy1 vlan 1-10
  ipv6 first hop security attach-policy policy2 vlan 12-20
```
Example 4—In the following example IPv6 First Hop Security detaches policy policy1 detached to the gi1/1/1 interface:

```
interface gi1/1/1
  no ipv6 first hop security attach-policy policy1
exit
```

59.16 ipv6 first hop security attach-policy (VLAN mode)

To attach an IPv6 First Hop Security policy to a specified VLAN, use the `ipv6 first hop security attach-policy` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ipv6 first hop security attach-policy policy-name

no ipv6 first hop security attach-policy
```

Parameters

`policy-name`—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration

The IPv6 First Hop Security default policy is applied.

Command Mode

Interface Configuration mode (VLAN)

User Guidelines

Use this command to attach an IPv6 First Hop Security policy to a VLAN.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Use the `no` form of the command to return to detach the current policy and to reattach the default policy. The `no` form of the command does not have an effect if the default policy was attached.
Example

In the following example, the IPv6 First Hop Security policy `policy1` is attached to VLAN 100:

```
interface vlan 100
  ipv6 first hop security attach-policy policy1
exit
```

59.17 ipv6 first hop security logging packet drop

To globally enable the logging of dropped packets by the IPv6 First Hop Security feature, use the `ipv6 first hop security logging packet drop` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ipv6 first hop security logging packet drop
no ipv6 first hop security logging packet drop
```

Parameters

N/A

Default Configuration

Logging is not enabled.

Command Mode

Global configuration

User Guidelines

Use this command to log packets that are dropped. If logging is enabled, the switch sends a rate-limited SYSLOG message every time it drops a message.

Example

The following example shows how to enable logging of dropped packets by the IPv6 first-hop security feature:
ipv6 first hop security logging packet drop

59.18 ipv6 first hop security policy
To define an IPv6 First Hop Security policy and place the switch in IPv6 First Hop Security Policy Configuration mode, use the \texttt{ipv6 first hop security policy} command in Global Configuration mode. To remove the IPv6 First Hop Security policy, use the \texttt{no} form of this command.

Syntax
\texttt{ipv6 first hop security policy policy-name}
\texttt{no ipv6 first hop security policy policy-name}

Parameters
\texttt{policy-name}—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration
No IPv6 First Hop Security policy is configured

Command Mode
Global configuration

User Guidelines
This command defines an IPv6 First Hop Security policy, and places the switch in IPv6 First Hop Security Policy Configuration mode

The following command can be configured in IPv6 First Hop Security Policy Configuration mode:

- \texttt{logging packet drop}

Each policy of the same type (for example, IPv6 First Hop Security policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports two predefined, empty, default IPv6 First Hop Security policies named: \texttt{"vlan_default"} and \texttt{"port_default"}:

\begin{verbatim}
ipv6 first hop security policy vlan_default
exit
ipv6 first hop security policy port_default
\end{verbatim}
exit

These policies cannot be removed but they can be changed. The no ipv6 first hop security policy does not remove these policies, it only removes the policy configurations defined by the user.

The default policies do not need to be attached by the ipv6 first hop security attach-policy command. The vlan_default policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The port_default policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the ipv6 first hop security policy command multiple times.

If an attached policy is removed, it is detached automatically before removing.

Examples

Example 1—The following example defines the IPv6 First Hop Security policy named policy1, places the switch in IPv6 First Hop Security Policy Configuration mode, and enables logging of dropped packets:

ipv6 first hop security policy policy1
  logging packet drop
exit

Example 2—The following example removes an attached IPv6 First Hop Security policy:

no ipv6 first hop security policy policy1

Policy policy1 is applied on the following interfaces:

  gi1/1/1, gi1/1/2

The policy1 will be detached and removed, are you sure [Y/N]Y

59.19 ipv6 nd inspection

To enable the IPv6 Neighbor Discovery (ND) Inspection feature on a VLAN, use the ipv6 nd inspection command in VLAN Configuration mode. To return to the default, use the no form of this command.
Syntax
ipv6 nd inspection
no ipv6 nd inspection

Parameters
N/A

Default Configuration
ND Inspection on a VLAN is disabled.

Command Mode
Interface Configuration mode (VLAN)

User Guidelines
Use the command to enable ND Inspection on a VLAN.
IPv6 ND Inspection validates the Neighbor Discovery Protocol (NDP) messages using the ND Inspection policies and global ND Inspection configuration.
ND Inspection bridges NDP messages to all interfaces excluding the source interface within the VLAN with the following exception: RS and CPS messages are not bridged to interfaces configured as host (see the device-role command).
ND inspection is performed after RA Guard.

Examples
Example 1—The following example enables ND Inspection on VLAN 100:

```
interface vlan 100
  ipv6 nd inspection
exit
```

Example 2—The following example enables ND Inspection on VLANs 100-107:

```
interface range vlan 100-107
  ipv6 nd inspection
```
To attach an ND Inspection policy to a specific interface, use the `ipv6 nd inspection attach-policy` command in Interface Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 nd inspection attach-policy policy-name [vlan vlan-list]
```

```
no ipv6 nd inspection attach-policy [policy-name]
```

**Parameters**

- `policy-name`—The ND Inspection policy name (up to 32 characters).
- `vlan vlan-list`—Specifies that the ND Inspection policy is to be attached to the VLAN(s) in `vlan-list`. If the `vlan` keyword is not configured, the policy is applied to all VLANs on the device on which ND Inspection is enabled.

**Default Configuration**

The ND Inspection default policy is applied.

**Command Mode**

Interface Configuration (Ethernet port or port channel).

**User Guidelines**

Use the `ipv6 nd inspection attach-policy` command to attach an ND Inspection policy to an interface.

Each succeeding usage of this command overrides the previous command with the same policy name.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Multiple policies with the `vlan` keyword can be attached to the same interface if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

a. The rules configured in the policy attached to the interface on the VLAN on which the packet arrived are added to the set.
b. The rules configured in the policy attached to the VLAN are added to the set if they have not been added.

c. The global rules are added to the set if they have not been added.

Use the `no ipv6 nd inspection attach-policy` command to detach all user-defined policies attached to the interface.

Use the `no ipv6 nd inspection attach-policy policy-name` command to detach the `policy-name` policy from the port.

**Examples**

**Example 1**—In the following example, the ND Inspection policy `policy1` is attached to the `gi1/1/1` interface:

```
interface gi1/1/1
  ipv6 nd inspection attach-policy policy1
exit
```

**Example 2**—In the following example, the ND Inspection policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and 12-20:

```
interface gi1/1/1
  ipv6 nd inspection attach-policy policy1 vlan 1-10,12-20
exit
```

**Example 3**—In the following example, the ND Inspection policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and the ND Inspection policy `policy2` is attached to the `gi1/1/1` interface and applied to VLANs 12-20:

```
interface gi1/1/1
  ipv6 nd inspection attach-policy policy1 vlan 1-10
  ipv6 nd inspection attach-policy policy2 vlan 12-20
exit
```
Example 4—In the following example, ND Inspection detaches policy policy1 from the gi1/1/1 interface:

```
interface gi1/1/1
   no ipv6 nd inspection attach-policy policy1
exit
```

### 59.21 ipv6 nd inspection attach-policy (VLAN mode)

To attach an ND Inspection policy to a specified VLAN, use the `ipv6 nd inspection attach-policy` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 nd inspection attach-policy policy-name

no ipv6 nd inspection attach-policy
```

**Parameters**

`policy-name`—The ND Inspection policy name (up to 32 characters).

**Default Configuration**

The ND Inspection default policy is applied.

**Command Mode**

Interface Configuration mode (VLAN)

**User Guidelines**

Use this command to attach a ND Inspection policy to a VLAN.

If the policy specified by the `policy-name` argument is not defined, the command is rejected.

Use the `no` form of the command to detach the current policy and to reattach the default policy. The `no` form of the command does not have an effect if the default policy was attached.
Example

In the following example, the ND Inspection policy, policy1, is attached to VLAN 100:

```
interface vlan 100
  ipv6 nd inspection attach-policy policy1
exit
```

### 59.22 ipv6 nd inspection drop-unsecure

To globally enable dropping messages with no CGA and RSA Signature options, use the `ipv6 nd inspection drop-unsecure` command in Global Configuration mode. To disable this function, use the `no` form of this command.

**Syntax**

```
ipv6 nd inspection drop-unsecure
no ipv6 nd inspection drop-unsecure
```

**Parameters**

N/A

**Default Configuration**

All messages are bridged.

**Command Mode**

Global configuration

**User Guidelines**

This command drops NDP messages if they do not contain CGA and RSA Signature options.

If this command is not configured, then the `sec-level minimum` command does not have an effect.

If this command is configured, then only the `sec-level minimum` command has an effect and all other configured ND Inspection policy commands are ignored.
Example

The following example enables the switch to drop messages with no or invalid options or an invalid signature:

```
ipv6 nd inspection drop-unsecure
```

59.23 ipv6 nd inspection policy

To define an ND Inspection policy and place the switch in IPv6 ND Inspection Policy Configuration mode, use the `ipv6 nd inspection policy` command in Global Configuration mode. To remove the ND Inspection policy, use the `no` form of this command.

Syntax

```
ipv6 nd inspection policy policy-name
no ipv6 nd inspection policy policy-name
```

Parameters

- `policy-name`—The ND Inspection policy name (up to 32 characters).

Default Configuration

No ND Inspection policies are configured.

Command Mode

Global Configuration

User Guidelines

This command defines the ND Inspection policy name, and places the router in ND Inspection Policy Configuration mode.

The following commands can be configured into a ND Inspection policy:

- `device-role` (ND Inspection Policy)
- `drop-unsecure`
- `sec-level minimum`
- `validate source-mac`
Each policy of the same type (for example, ND Inspection policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined ND Inspection policies named: "vlan_default" and "port_default":

```
ipv6 nd inspection policy vlan_default
exit
ipv6 nd inspection policy port_default
exit
```

These policies cannot be removed, but they can be changed. The `no ipv6 nd inspection policy` does not remove these policies, it only removes the policy configuration defined by the user.

The default policies cannot be attached by the `ipv6 nd inspection attach-policy` command. The `vlan_default` policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The `port_default` policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the `ipv6 nd inspection policy` command multiple times.

If an attached policy is removed it is detached automatically before removing.

**Examples**

**Example 1.** The following example defines a ND Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and configures the port to drop unsecured messages and sets the device role as router:

```
ipv6 nd inspection policy policy1
  drop-unsecure
  device-role router
exit
```

**Example 2.** The following example defines an ND Inspection policy as policy1 by a few steps:

```
ipv6 nd inspection policy policy1
  drop-unsecure
```
exit

ipv6 nd inspection policy policy1
    device-role router

exit

Example 3. The following example removes an attached ND Inspection policy:

no ipv6 nd inspection policy policy1

Policy policy1 is applied on the following interfaces:

    gi1/1/1, gi1/1/2

The policy1 will be detached and removed, are you sure [Y/N]Y

59.24 ipv6 nd inspection sec-level minimum

To globally specify the minimum security level value, use the ipv6 nd inspection sec-level minimum command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

ipv6 nd inspection sec-level minimum value

no ipv6 nd inspection sec-level minimum

Parameters

value—Sets the minimum security level. Range: 0–7.

Default Configuration

All messages are bridged.

Command Mode

Global configuration

User Guidelines

This command specifies the minimum security level parameter value when the drop-unsecured feature is configured.
This command has no effect if dropping of non secure messages is not enabled.

Example

The following example enables the switch to specify 2 as the minimum CGA security level:

```
ipv6 nd inspection sec-level minimum 2
```

### 59.25 ipv6 nd inspection validate source-mac

To globally enable checking source MAC address against the link-layer address in the source/target link layer option, use the `ipv6 nd inspection validate source-mac` command in Global Configuration mode. To disable this function, use the `no` form of this command.

**Syntax**

```
ipv6 nd inspection validate source-mac
no ipv6 nd inspection validate source-mac
```

**Parameters**

N/A

**Default Configuration**

This command is disabled by default.

**Command Mode**

Global configuration

**User Guidelines**

When the switch receives an NDP message, which contains a link-layer address in the source/target link layer option, the source MAC address is checked against the link-layer address. Use this command to drop the packet if the link-layer address and the MAC addresses are different from each other.
Example

The following example enables the switch to drop an NDP message whose link-layer address in the source/target link layer option does not match the MAC address:

```
ipv6 nd inspection validate source-mac
```

### 59.26 ipv6 nd raguard

To globally enable the router advertisements (RA) guard feature on a VLAN, use the `ipv6 nd raguard` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 nd raguard

no ipv6 nd raguard
```

**Parameters**

N/A

**Default Configuration**

RA Guard on a VLAN is disabled.

**Command Mode**

Interface Configuration mode (VLAN)

**User Guidelines**

Use the `ipv6 nd raguard` command, to enable IPv6 RA Guard on a VLAN.

RA Guard discards RA, CPA, and ICMP Redirect messages received on interfaces that are not configured as router (see the `device-role` command).

RA Guard validates received RA messages based on an RA Guard policy attached to the source interface.

RA Guard is performed before ND inspection.
Examples

Example 1—The following example enables RA Guard on VLAN 100:

```plaintext
interface vlan 100
  ipv6 nd raguard
exit
```

Example 2—The following example enables RA Guard on VLANs 100-107:

```plaintext
interface range vlan 100-107
  ipv6 nd raguard
exit
```

59.27  ipv6 nd raguard attach-policy (port mode)

To attach an RA Guard policy to a specific interface, use the `ipv6 nd raguard attach-policy` command in Interface Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```plaintext
ipv6 nd raguard attach-policy policy-name [vlan vlan-list]
no ipv6 nd raguard attach-policy [policy-name]
```

Parameters

- `policy-name`—The RA Guard policy name (up to 32 characters).
- `vlan vlan-list`—Specifies that the RA Guard policy is to be attached to the VLAN(s) in `vlan-list`. If the `vlan` keyword is not configured, the policy is applied to all VLANs on the device on which RA Guard policy is enabled.

Default Configuration

The RA Guard default policy is applied.

Command Mode

Interface Configuration (Ethernet port or port channel).
User Guidelines

Use this command to attach an RA Guard policy to an interface.

Each succeeding `ipv6 nd raguard attach-policy` command overrides the previous command with the same policy.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Multiple policies with the `vlan` keyword can be attached to the same interface if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

a. The rules configured in the policy attached to the interface on the VLAN on which the packet arrived are added to the set.

b. The rules configured in the policy attached to the VLAN are added to the set if they have not been added.

c. The global rules are added to the set if they have not been added.

Use the `no ipv6 nd raguard attach-policy` command to detach all user-defined policies attached to the interface.

Use the `no ipv6 nd raguard attach-policy policy-name` command to detach the `policy-name` policy from the port.

Examples

Example 1—In the following example, the RA Guard policy `policy1` is attached to the `gi1/1/1` interface:

```plaintext
interface gi1/1/1
    ipv6 nd raguard attach-policy policy1
exit
```

Example 2—In the following example, the RA Guard policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and 12-20:

```plaintext
interface gi1/1/1
    ipv6 nd raguard attach-policy policy1 vlan 1-10,12-20
exit
```
Example 3—In the following example, the RA Guard policy `policy1` is attached to the `gi1/1/1` interface and applied to VLANs 1-10 and the RA Guard policy `policy2` is attached to the `gi1/1/1` interface and applied to VLANs 12-20:

```plaintext
interface gi1/1/1
  ipv6 nd raguard attach-policy policy1 vlan 1-10
  ipv6 nd raguard attach-policy policy2 vlan 12-20
exit
```

Example 4—In the following example RA Guard detaches policy `policy1` from the `gi1/1/1` interface:

```plaintext
interface gi1/1/1
  no ipv6 nd raguard attach-policy policy1
exit
```

### 59.28 ipv6 nd raguard attach-policy (VLAN mode)

To attach an RA Guard policy to a specified VLAN, use the `ipv6 nd raguard attach-policy` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```plaintext
ipv6 nd raguard attach-policy policy-name

no ipv6 nd raguard attach-policy
```

**Parameters**

`policy-name`—The RA Guard policy name (up to 32 characters).

**Default Configuration**

The RA Guard default policy is applied.

**Command Mode**

Interface Configuration mode (VLAN)
User Guidelines

Use this command to attach an RA Guard policy to a VLAN.

If a policy specified by the policy-name argument is not defined, the command is rejected.

Use the no form of the command to rdetach the current policy and to reattach the default policy. The no form of the command has no effect if the default policy was attached.

Example

In the following example, the RA Guard policy policy1 is attached to VLAN 100:

```
interface vlan 100
  ipv6 nd raguard attach-policy policy1
exit
```

59.29 ipv6 nd raguard hop-limit

To globally enable verification of the advertised Cur Hop Limit value in RA messages, use the `ipv6 nd raguard hop-limit` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

```
ipv6 nd raguard hop-limit {maximum value} {minimum value}
no ipv6 nd raguard hop-limit [maximum] [minimum]
```

Parameters

- `maximum value`—Verifies that the hop-count limit is lower than or equal to the `value` argument. Range 1-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- `minimum value`—Verifies that the hop-count limit is greater than or equal to the `value` argument. Range 1-255.

Default Configuration

No hop-count limit is verified.
Command Mode
Global configuration

User Guidelines
This command enables verification that the advertised Cur Hop Limit value in an RA message (see RFC4861) is greater than or less than the value set by the value argument.

Configuring the minimum value keyword and argument can prevent an attacker from setting a low Cur Hop Limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the maximum value keyword and argument enables verification that the advertised Cur Hop Limit value is lower than or equal to the value set by the value argument. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Use the no ipv6 nd raguard hop-limit maximum command to disable verification of the maximum boundary of the advertised Cur Hop Limit value in an RA message.

Use the no ipv6 nd raguard hop-limit minimum command to disable verification of the minimum boundary of the advertised Cur Hop Limit value in an RA message.

Examples
Example 1—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using two commands:

```
ipv6 nd raguard hop-limit minimum 3
ipv6 nd raguard hop-limit maximum 100
```

Example 2—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using a single command:

```
ipv6 nd raguard hop-limit minimum 3 maximum 100
```

59.30 ipv6 nd raguard managed-config-flag
To globally enable verification of the advertised “Managed address configuration” flag in RA messages, use the ipv6 nd raguard managed-config-flag command in
Global Configuration mode. To return to the default, use the no form of this command.

Syntax

ipv6 nd raguard managed-config-flag {on | off}
no ipv6 nd raguard managed-config-flag

Parameters

- on—The value of the flag must be 1.
- off—The value of the flag must be 0.

Default Configuration

Verification is not enabled.

Command Mode

Global configuration

User Guidelines

This command enables verification of the advertised “Managed Address Configuration” flag (or "M" flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that might not be trustworthy.

Example

The following example enables M flag verification that checks if the value of the flag is 0:

```
ipv6 nd raguard managed-config-flag off
```

59.31 ipv6 nd raguard other-config-flag

To globally enable verification of the advertised “Other Configuration” flag in RA messages, use the ipv6 nd raguard other-config-flag command in Global Configuration mode. To return to the default, use the no form of this command.
Syntax
ipv6 nd raguard other-config-flag {on | off}
no ipv6 nd raguard other-config-flag

Parameters
- on—The value of the flag must be 1.
- off—The value of the flag must be 0.

Default Configuration
Verification is not enabled.

Command Mode
Global configuration

User Guidelines
This command enables verification of the advertised “Other Configuration” flag (or "O" flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to retrieve other configuration information through a DHCPv6 server that might not be trustworthy.

Example
The following example shows how the command enables O flag verification that checks if the value of the flag is 0:

```
ipv6 nd raguard other-config-flag off
```

59.32 ipv6 nd raguard policy

To define an RA Guard policy name and place the switch in IPv6 RA Guard Policy Configuration mode, use the `ipv6 nd raguard policy policy-name` command in Global Configuration mode. To remove the RA Guard policy, use the `no` form of this command.

Syntax
ipv6 nd raguard policy policy-name
no ipv6 nd raguard policy policy-name
Parameters

policy-name—The RA Guard policy name (up to 32 characters).

Default Configuration

No RA Guard policy are configured

Command Mode

Global configuration

User Guidelines

This command defines the RA Guard policy name, and places the switch in IPv6 RA Guard Policy Configuration mode.

Each policy of the same type (for example, RA Guard policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined RA Guard policies, named: "vlan_default" and "port_default":

```
ipv6 nd raguard policy vlan_default
exit

ipv6 nd raguard policy port_default
exit
```

The policies cannot be removed, but they can be changed. The no ipv6 nd raguard policy does not remove these policies, it only removes the policy configuration defined by the user.

The policies cannot be attached by the ipv6 nd raguard attach-policy command. The vlan_default policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The port_default policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the ipv6 nd raguard policy command multiple times.

If an attached policy is removed, it is detached automatically before removing.

The following commands can be configured in RA Guard Policy Configuration mode:

- device-role (RA Guard Policy)
- hop-limit
- managed-config-flag
Examples

Example 1—The following example defines an RA Guard policy named policy1, places the router in RA Guard Policy Configuration mode, and disenables validation of "Other Configuration" flag, and sets the device role as router:

```
ipv6 nd raguard policy policy1
  other-config-flag disable
  device-role router
exit
```

Example 2—The following example defines an RA Guard named policy1 using multiple steps:

```
ipv6 nd raguard policy policy1
  other-config-flag disable
exit
ipv6 nd raguard policy policy1
  device-role router
exit
```

Example 3—The following example removes an attached RA Guard policy:

```
no ipv6 nd raguard policy policy1
```

Policy policy1 is applied on the following interfaces:

```
gi1/1/1, gi1/1/2
```

The policy1 will be detached and removed, are you sure [Y/N]? Y
59.33  ipv6 nd raguard router-preference

To globally enable verification of the advertised Default Router Preference value in RA messages, use the `ipv6 nd raguard router-preference` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

`ipv6 nd raguard router-preference {maximum value} {minimum value}`

`no ipv6 nd raguard router-preference {maximum} {minimum}`

Parameters

- `maximum value`—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191). The value of the high boundary must be equal to or greater than the value of the low boundary.

- `minimum value`—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).

Default Configuration

Verification is not enabled.

Command Mode

Global configuration

User Guidelines

This command enables verification of the advertised Default Router Preference value in RA messages (see RFC4191).

Configuring the `minimum value` keyword and argument specifies the minimum allowed value. Received RA messages with a Default Router Preference value less than the `value` argument are dropped.

Configuring the `maximum value` keyword and argument specifies the maximum allowed value. Received RA messages with a Default Router Preference value greater than the `value` argument are dropped.

Use the `no ipv6 nd raguard router-preference` command to disable verification of the advertised Default Router Preference value in RA messages.
Use the `no ipv6 nd raguard router-preference maximum` command to disable verification of the maximum boundary of the advertised Default Router Preference value in RA messages.

Use the `no ipv6 nd raguard router-preference minimum` command to disable verification of the advertised Default Router Preference value in RA messages.

**Examples**

**Example 1**—The following example defines that only a value of *medium* is acceptable using two commands:

```
ipv6 nd raguard router-preference minimum medium
ipv6 nd raguard router-preference maximum medium
```

**Example 2**—The following example defines that only a value of *medium* is acceptable using a single command:

```
ipv6 nd raguard router-preference minimum medium maximum medium
```

### 59.34 ipv6 neighbor binding

To globally enable the Neighbor Binding (NB) integrity feature on a VLAN, use the `ipv6 neighbor binding` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 neighbor binding
no ipv6 neighbor binding
```

**Parameters**

N/A

**Default Configuration**

NB integrity on a VLAN is disabled.

**Command Mode**

Interface Configuration mode (VLAN)
User Guidelines

NB integrity establishes binding for neighbors connected to the perimetrical ports (see the device-role (Neighbor Binding) command) belonging to the VLANs on which the feature is enabled.

Examples

Example 1—The following example enables NB integrity on VLAN 100:

```plaintext
interface vlan 100
  ipv6 neighbor binding
exit
```

Example 2—The following example enables NB integrity on VLANs 100-107:

```plaintext
interface range vlan 100-107
  ipv6 neighbor binding
exit
```

59.35 ipv6 neighbor binding attach-policy (port mode)

To attach a Neighbor Binding policy to a specific interface, use the ipv6 neighbor binding attach-policy command in Interface Configuration mode. To return to the default, use the no form of this command.

Syntax

```
ipv6 neighbor binding attach-policy policy-name [vlan vlan-list]
no ipv6 neighbor binding attach-policy [policy-name]
```

Parameters

- `policy-name`—The Neighbor Binding policy name (up to 32 characters).
- `vlan vlan-list`—Specifies that the Neighbor Binding policy is to be attached to the VLAN(s) in `vlan-list`. If the `vlan` keyword is not configured, the policy is applied to all VLANs on the device on which Neighbor Binding policy is enabled.
Default Configuration
The Neighbor Binding default policy is applied.

Command Mode
Interface Configuration (Ethernet port or port channel).

User Guidelines
Use this command to attach a Neighbor Binding policy to an interface.

Each succeeding `ipv6 neighbor binding attach-policy` command overrides the previous command with the same policy.

If a policy specified by the `policy-name` argument is not defined, the command is rejected.

Multiple policies with the `vlan` keyword can be attached to the same interface if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

a. The rules configured in the policy attached to the interface on the VLAN on which the packet arrived are added to the set.

b. The rules configured in the policy attached to the VLAN are added to the set if they have not been added.

c. The global rules are added to the set if they have not been added.

Use the `no ipv6 neighbor binding attach-policy` command to detach all user-defined policies attached to the interface.

Use the `no ipv6 neighbor binding attach-policy policy-name` command to detach the `policy-name` policy from the port.

Examples
Example 1—In the following example, the Neighbor Binding policy `policy1` is attached to the `gi1/1/1` interface:

```
interface gi1/1/1
  ipv6 neighbor binding attach-policy policy1
exit
```
Example 2—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/1/1 interface and applied to VLANs 1-10 and 12-20:

```plaintext
interface gi1/1/1
  ipv6 neighbor binding attach-policy policy1 vlan 1-10,12-20
exit
```

Example 3—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/1/1 interface and applied to VLANs 1-10, and the ND Inspection policy policy2 is attached to the gi1/1/1 interface and applied to VLANs 12-20:

```plaintext
interface gi1/1/1
  ipv6 neighbor binding attach-policy policy1 vlan 1-10
  ipv6 neighbor binding attach-policy policy2 vlan 12-20
exit
```

Example 4—In the following example, Neighbor Binding Integrity detaches policy policy1 detached to the gi1/1/1 interface:

```plaintext
interface gi1/1/1
  no ipv6 neighbor binding attach-policy policy1
exit
```

### 59.36 ipv6 neighbor binding attach-policy (VLAN mode)

To attach a Neighbor Binding policy to a specific VLAN, use the `ipv6 neighbor binding attach-policy` command in VLAN Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
ipv6 neighbor binding attach-policy policy-name

no ipv6 neighbor binding attach-policy
```
Parameters

*policy-name*—The Neighbor Binding policy name (up to 32 characters).

Default Configuration

The Neighbor Binding default policy is applied.

Command Mode

Interface Configuration mode (VLAN)

User Guidelines

Use this command to attach a Neighbor Binding policy to a VLAN.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Use the no form of the command to return to detach the current policy and reattach the default policy. The no form of the command has no effect if the default policy was attached.

Example

In the following example, the Neighbor Binding policy *policy1* is attached to VLAN 100:

```
interface vlan 100
  ipv6 neighbor binding attach-policy policy1
exit
```

59.37  ipv6 neighbor binding lifetime

To globally change the default of the Neighbor Binding table entry lifetime, use the *ipv6 neighbor binding lifetime* command in Global Configuration mode. To return to the default setting, use the no form of this command.

Syntax

```
ipv6 neighbor binding lifetime value
no ipv6 neighbor binding lifetime
```
Parameters

value—The lifetime in minutes. The range is from 1 through 60 minutes.

Default Configuration

5 minutes

Command Mode

Global configuration

User Guidelines

Use the ipv6 neighbor binding lifetime command to change the default lifetime.

Example

The following example changes the lifetime for binding entries to 10 minutes:

```
ipv6 neighbor binding lifetime 10
```

59.38 ipv6 neighbor binding logging

To globally enable the logging of Binding table main events, use the ipv6 neighbor binding logging command in Global Configuration mode. To disable this feature, use the no form of this command.

Syntax

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

Parameters

N/A

Default Configuration

Binding table events are not logged.

Command Mode

Global configuration
User Guidelines

This command enables the logging of the following Binding table events:

- An entry is inserted into the Binding table.
- A Binding table entry was updated.
- A Binding table entry was deleted from the Binding table.
- A Binding table entry was not inserted into the Binding table, possibly because the maximum number of entries has been reached or because of Binding table overflow.

Example

The following example shows how to enable Binding table event logging:

```
ipv6 neighbor binding logging
```

59.39 ipv6 neighbor binding max-entries

To globally specify the maximum number of dynamic entries that are allowed to be inserted in the Binding table cache, use the `ipv6 neighbor binding max-entries` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ipv6 neighbor binding max-entries [[vlan-limit number] [interface-limit number] [mac-limit number]]
```

```
o ipv6 neighbor binding max-entries [vlan-limit] [interface-limit] [mac-limit]
```

Parameters

- `vlan-limit number`—Specifies a neighbor binding limit per number of VLANs.
- `interface-limit number`—Specifies a neighbor binding limit per interface.
- `mac-limit number`—Specifies a neighbor binding limit per MAC address.

Default Configuration

This command is disabled.
Command Mode

Global configuration

User Guidelines

This command is used to control the contents of the Binding table. This command specifies the maximum number of dynamic entries that can be inserted in the Binding table cache. After this limit is reached, new entries are refused, and a Neighbor Discovery Protocol (NDP) traffic source with a new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

Example

The following example shows how to specify globally the maximum number of entries that can be inserted into the cache per MAC:

```
ipv6 neighbor binding max-entries mac-limit 2
```

59.40 ipv6 neighbor binding policy

To define a Neighbor Binding policy and place the switch in IPv6 Neighbor Binding Policy Configuration mode, use the `ipv6 neighbor binding policy` command in Global Configuration mode. To remove the Neighbor Binding policy, use the `no` form of this command.

Syntax

```
ipv6 neighbor binding policy policy-name
no ipv6 neighbor binding policy policy-name
```

Parameters

```
policy-name—The Neighbor Binding policy name (up to 32 characters).
```

Default Configuration

No Neighbor Binding policy is configured

Command Mode

Global configuration
User Guidelines

This command defines a Neighbor Binding policy name, and places the router in Neighbor Binding Policy Configuration mode so that additional commands can be added to the policy.

The switch supports two predefined Neighbor Binding policies, named: "vlan_default" and "port_default":

```
ipv6 neighbor binding policy vlan_default
exit

ipv6 neighbor binding policy port_default
exit
```

The policies cannot be removed, but they can be changed. The no ipv6 neighbor binding policy does not remove these policies, it only removes the policy configuration defined by the user.

The policies cannot be attached by the ipv6 neighbor binding attach-policy command. The vlan_default policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The port_default policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the ipv6 neighbor binding policy command multiple times.

If an attached policy is removed, it is detached automatically before removing.

The following commands can be configured into IPv6 Neighbor Binding Policy Configuration mode:

- device-role (Neighbor Binding)
- logging binding
- max-entries

Examples

Example 1—The following example defines a Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, enables logging, and defines the port as internal:

```
ipv6 neighbor binding policy policy1
  device-role internal
  logging binding
```
Example 2—The following example defines a Neighbor Binding policy named policy1 using multiple steps:

```
ipv6 neighbor binding policy policy1
  device-role internal
exit
ipv6 neighbor binding policy policy1
  logging binding
exit
```

Example 3—The following example remove an attached Neighbor Binding policy:

```
no ipv6 neighbor binding policy policy1
```

Policy policy1 is applied on the following interfaces:

```
gi1/1/1, gi1/1/2
```

The policy1 will be detached and removed, are you sure [Y/N] Y

59.41 ipv6 neighbor binding static

To add a static entry to the Neighbor Binding table, use the `ipv6 neighbor binding static` command in Global Configuration mode. To remove the static entry, use the `no` form of this command.

**Syntax**

```
ipv6 neighbor binding static ipv6 ipv6-address vlan vlan-id interface interface-id mac mac-address
```

```
no ipv6 neighbor binding static ipv6 ipv6-address vlan vlan-id
```

**Parameters**

- `ipv6 ipv6-address`—IPv6 address of the static entry.
- `vlan vlan-id`—ID of the specified VLAN.
- `interface interface-id`—Adds static entries to the specified interface.
- `mac mac-address`—MAC address of the static entry.

**Default Configuration**

No static entry.

**Command Mode**

Global configuration

**User Guidelines**

This command is used to add static entries to the Neighbor Binding table. Static entries can be configured regardless the port role.

If the entry (dynamic or static) already exists, the new static entry overrides the existing one.

If the Neighbor Binding table overflows, the static entry is not added.

**Example**

The following example adds a static entry:

```
ipv6 neighbor binding static ipv6 2001:600::1 vlan 100 interface gi1/1/1 mac 00BB.CC01.F500
```

**59.42 logging binding**

To enable the logging of Binding table main events within an IPv6 Neighbor Binding policy, use the `logging binding` command in Neighbor Binding Policy Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```plaintext
logging binding [enable | disable]
```

```plaintext
no logging binding
```
Parameters

- **enable**—Enables logging of Binding table main events. If no keyword is configured, the keyword is applied by default.
- **disable**—Disables logging of Binding table main events.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration (config-nbr-binding)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of Binding table main events within the IPv6 Neighbor Binding policy named policy1:

```
ipv6 neighbor binding policy policy1
  logging binding enable
exit
```

59.43 logging packet drop

To enable the logging of dropped packets within an IPv6 First Hop Security policy, use the **logging packet drop** command in IPv6 First Hop Security Policy Configuration mode. To return to the default, use the no form of this command.

Syntax

- **logging packet drop [enable | disable]**
- **no logging packet drop**
Parameters

- **enable**—Enables logging of dropped packets. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables logging of dropped packets.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

IPv6 First Hop Security Policy Configuration mode (config-ipv6-fhs)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of dropped messages with the IPv6 First Hop Security Policy named policy1:

```
ip6 first hop security policy policy1
   logging packet drop
exit
```

59.44 managed-config-flag

To enable verification of the advertised Managed Address Configuration flag within an IPv6 RA Guard policy, use the `managed-config-flag` command in RA Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
managed-config-flag {on | off | disable}
```

```
no managed-config-flag
```
Parameters

- on—The value of the flag must be 1.
- off—The value of the flag must be 0.
- disable—The value of the flag is not validated.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration (config-ra-guard)

User Guidelines

Use this command to change the global configuration specified by the ipv6 nd raguard managed-config-flag command on the port on which this policy applies.

Use the disable keyword to disable the flag validation in both global or the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and enables M flag verification that checks if the value of the flag is 0:

```
ipv6 nd raguard policy policy1
    managed-config-flag off
exit
```

59.45 match ra address

To enable verification of the router's IPv6 address in received RA messages within an IPv6 RA Guard policy, use the match ra address command in RA Guard Policy Configuration mode. To return to the default, use the no form of this command.
Syntax
match ra address {prefix-list ipv6-prefix-list-name} | disable
no match ra address

Parameters
- prefix-list ipv6-prefix-list-name—The IPv6 prefix list to be matched.
- disable—Disables verification of the router’s IPv6 address.

Default Configuration
Policy attached to port or port channel: the value configured in the policy attached to the VLAN.
Policy attached to VLAN: router’s addresses are not verified.

Command Mode
RA Guard Policy Configuration (config-ra-guard)

User Guidelines
This command enables verification of the router’s IPv6 address in received RA messages by a configured prefix list. If the router’s source IPv6 address does not match the prefix list or if the prefix list is not configured, the RA message is dropped.

Use the disable keyword to disable verification of the router’s IPv6 address regardless of the VLAN configuration.

Example
The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, matches the router addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the router with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
ipv6 nd raguard policy policy1
  match ra address prefix-list list1
exit
ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```
59.46 match ra prefixes

To enable verification of the advertised prefixes in received RA messages within an IPv6 RA Guard policy, use the `match ra prefixes` command in RA Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
match ra prefixes [prefix-list ipv6-prefix-list-name] | disable
no match ra prefixes
```

Parameters

- `prefix-list ipv6-prefix-list-name`—The IPv6 prefix list to be matched.
- `disable`—Disables verification of the advertised prefixes in received RA messages.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: advertised prefixes are not verified.

Command Mode

RA Guard Policy Configuration (config-ra-guard)

User Guidelines

This command enables verification of the advertised prefixes in received RA messages by a configured prefix list. If an advertised prefix does not match the prefix list, or if the prefix list is not configured, the RA message is dropped.

Use the `disable` keyword to disable verification of the advertised prefixes in received RA messages in both global or the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard configuration mode, matches the prefixes to the prefix list named list1, and the 2001:10::/64 prefixes and denies 2001:100::/64 prefixes:

```
ipv6 nd raguard policy policy1
```
IPv6 First Hop Security

match ra prefixes prefix-list list1
exit
ipv6 prefix-list list1 deny 2001:0DB8:101::/64
ipv6 prefix-list list1 permit 2001:0DB8:100::/64

59.47 match reply

To enable verification of the assigned IPv6 addresses in messages sent by DHCPv6 servers/relays to a configured prefix list within a DHCPv6 Guard policy, use the match reply command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the no form of this command.

Syntax
match reply [prefix-list ipv6-prefix-list-name] | disable
no match reply

Parameters
- ipv6-prefix-list-name—The IPv6 prefix list to be matched.
- disable—Disables verification of the advertised prefixes in replies.

Default Configuration
Policy attached to port or port channel: the value configured in the policy attached to the VLAN.
Policy attached to VLAN: advertised prefixes are not verified.

Command Mode
DHCPv6 guard Policy Configuration (config-dhcpv6-guard)

User Guidelines
IPv6 DHCP Guard verifies the assigned IPv6 addresses to the configure prefix list passed in the IA_NA and IA_TA options of the following DHCPv6 messages sent by DHCPv6 servers/relays:
- ADVERTISE
- REPLY
- RELAY-REPL
Note 1. Assigned addresses are not verified if a value of the Status Code option (if it presents) differs from the following ones:

- Success
- UseMulticast

Note 2. In RELAY-REPL messages DHCPv6 Guard validates the message encapsulated in the DHCP-relay-message option.

Use the `disable` keyword to disable verification of the assigned IPv6 addresses in replies.

Example

The following example defines a DHCPv6 Guard policy named `policy1`, places the switch in DHCPv6 Guard policy configuration mode, matches the assigned addresses to the prefix list named `list1`: all assigned IPv6 addresses must belong to 2001:0DB8:100:200/64 or to 2001:0DB8:100::/48. The "ge 128" parameter must be configured for each prefix of the prefix-list with prefix length less than 128.

```
ipv6 dhcp guard policy policy1
  match reply prefix-list list1
exit
ipv6 prefix-list list1 deny 2001:0DB8:100:200/64 ge 128
ipv6 prefix-list list1 permit 2001:0DB8:100::/48 ge 128
```

59.48 match server address

To enable verification of the source IPv6 address in messages sent by DHCPv6 servers or DHCPv6 Relays to a configured prefix list within a DHCPv6 Guard policy, use the `match server address` command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`match server address [prefix-list ipv6-prefix-list-name] | disable`

`no match server address`

Parameters

- `prefix-list ipv6-prefix-list-name`—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the DHCP server's and relay's IPv6 address.

**Default Configuration**

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: server's addresses are not verified.

**Command Mode**

DHCP guard Policy Configuration (config-dhcp-guard)

**User Guidelines**

This command enables verification of the source IPv6 address in messages sent by DHCPv6 servers and DHCPv6 Relays to a configured prefix list. If the source IPv6 address does not match to the configured prefix list or if the prefix list is not configured, the DHCPv6 reply message, the message is dropped.

IPv6 DHCP Guard verifies the source IPv6 address in the following DHCPv6 messages sent by DHCPv6 servers/relays:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

Use the **disable** keyword to disable verification of the DHCP server's and relay's IPv6 address.

**Example**

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, matches the server or relay addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the server with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
ipv6 dhcp guard policy policy1
  match server address prefix-list list1
exit
```
ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128

59.49 max-entries

To define the maximum number of dynamic entries that can be inserted in the Binding table cache within an IPv6 Neighbor Binding policy, use the `max-entries` command in Neighbor Binding Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
max-entries { [vlan-limit { number | disable }] [interface-limit { number | disable }] [mac-limit { number | disable }] }
```

```
no max-entries [vlan-limit] [interface-limit] [mac-limit]
```

Parameters

- `vlan-limit number`—Specifies a neighbor binding limit per VLANs. The parameter is ignored in a policy attached to port.
- `vlan-limit disable`—Disables a neighbor binding limit per VLANs.
- `interface-limit number`—Specifies a neighbor binding limit per interface.
- `interface-limit disable`—Disables a neighbor binding limit per interface.
- `mac-limit number`—Specifies a neighbor binding limit per MAC address.
- `mac-limit disable`—Disables a neighbor binding limit per MAC address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration (config-nbr-binding)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.
Examples

Example 1—The following example defines an Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
ipv6 neighbor binding policy policy1
    max-entries interface-limit 25
exit
```

Example 2—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables limit per MAC:

```
ipv6 nd raguard policy policy1
    max-entries mac-limit disable
exit
```

59.50 other-config-flag

To enable the verification of the advertised “Other Configuration” flag in RA messages within an IPv6 RA Guard policy, use the `other-config-flag` command in RA Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
other-config-flag {on | off | disable}
```

```
no other-config-flag
```

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.
- **disable**—The value of the flag is not validated.
Default Configuration
Policy attached to port or port channel: the value configured in the policy attached to the VLAN.
Policy attached to VLAN: global configuration.

Command Mode
RA Guard Policy Configuration (config-ra-guard)

User Guidelines
Use this command to change the global configuration specified by the `ipv6 nd raguard other-config-flag` command on the port on which this policy applies.

Use the `disable` keyword to disable flag validation in both global or VLAN configuration.

Example
The following example defines an RA Guard policy named `policy1`, places the switch in RA Guard Policy Configuration mode, and enables O flag verification that checks if the value of the flag is 0:

```
ipv6 nd raguard policy policy1
    other-config-flag off
exit
```

59.51 preference
To enable verification of the preference in messages sent by DHCPv6 servers within a DHCPv6 Guard policy, use the `preference` command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the no form of this command.

Syntax
```
preference {[maximum {value|disable}] [minimum {value|disable}]}
no preference [maximum] [minimum]
```
Parameters

- **maximum value**—Advertised preference value is lower or equal than that set by the value argument. Range 0-255. A value of the high boundary must be equal to or greater than a value of the low boundary.

- **maximum disable**—Disables verification of the high boundary of the advertised preference value.

- **minimum value**—Advertised preference value is greater than or equal to the value argument. Range 0-255.

- **minimum disable**—Disables verification of the lower boundary of the advertised preference value.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

DHCP guard Policy Configuration (config-dhcp-guard)

User Guidelines

Use this command to change the global configuration specified by the `ipv6 dhcp guard preference` command on the port on which this policy applies.

Use the `disable` keyword to disable verification in both global or VLAN configuration.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, and defines a minimum preference value of 10:

```
ipv6 dhcp guard policy policy1
  preference minimum 10
exit
```
59.52 router-preference

To enable verification of advertised Default Router Preference value in RA messages within an IPv6 RA Guard policy, use the `router-preference` command in RA Guard Policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
router-preference [maximum {value | disable}] [minimum {value | disable}]
no router-preference [maximum] [minimum]
```

Parameters

- `maximum value`—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: `low`, `medium` and `high` (see RFC4191). A value of the high boundary must be equal to or greater than a value of the low boundary.
- `maximum disable`—Disables verification of the high boundary of Advertised Default Router Preference.
- `minimum value`—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: `low`, `medium` and `high` (see RFC4191).
- `minimum disable`—Disables verification of the low boundary of Advertised Default Router Preference.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration (config-ra-guard)

User Guidelines

Use this command to change the global configuration specified by the `ipv6 nd raguard router-preference` command on the port on which this policy applies.

Use the `disable` keyword to disable of verification in both global or VLAN configuration.
Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Default Router Preference value of medium:

```
ipv6 nd raguard policy policy1
    router-preference minimum medium
exit
```

59.53 sec-level minimum

To specify the minimum security level value within an IPv6 ND Inspection policy, use the `sec-level minimum` command in ND Inspection policy Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
sec-level minimum value | disable
no sec-level minimum
```

Parameters

- **value**—Sets the minimum security level, which is a value from 0 through 7.
- **disable**—Disables verification of security level parameter

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND Inspection Policy Configuration (config-nd-inspection)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.
This command has no effect if dropping of unsecured messages is not enabled.

Example

The following example defines an NDP Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and specifies 2 as the minimum CGA security level:

```
ipv6 nd inspection policy policy1
  sec-level minimum 2
exit
```

59.54  `show ipv6 dhcp guard`

To display DHCPv6 Guard global configuration, use the `show ipv6 dhcp guard` command in Privilege EXEC configuration mode.

Syntax

```
show ipv6 dhcp guard
```

Parameters

N/A

Command Mode

Privilege EXEC configuration mode

User Guidelines

The `show ipv6 dhcp guard` command displays DHCPv6 Guard global configuration.

Example

The following example gives an example of the output of the `show ipv6 dhcp guard` command:

```
show ipv6 dhcp guard
IPv6 DHCP Guard is enabled on VLANs:1-4,6,7,100-120
Default Preference
```
minimum: 10
maximum: 100

59.55  show ipv6 dhcp guard policy

To display DHCPv6 guard policies on all interfaces configured with the DHCPv6 guard feature, use the `show ipv6 dhcp guard policy` command in privileged EXEC mode.

Syntax

`show ipv6 dhcp guard policy [policy-name]`

Parameters

- `policy-name`—Displays the DHCPv6 guard policy with the given name.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command displays the options configured for the policy on all interfaces configured with the DHCPv6 guard feature.

Examples

Example 1—The following example shows the Policy Configuration for a policy named policy1:

```bash
show ipv6 dhcp guard policy policy1
DHCPv6 Guard Policy: policy1
   device-role: server
   preference
      minimum: 1 (from policy2 attached to the VLAN)
      maximum: 200 (from policy2 attached to the VLAN)
   server address prefix list: list1
   reply prefix list name: list10
   Attached to VLANs: 1-100,111-4094
```
Attached to ports:

<table>
<thead>
<tr>
<th>Interface</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ge1/0/5-7</td>
<td>1-58, 68-4094</td>
</tr>
<tr>
<td>Ge1/0/8-24, Ge2/0/1-24</td>
<td>1-4094</td>
</tr>
<tr>
<td>Po1-4</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Example 2—The following example shows the attached policies:

```
show ipv6 dhcp guard policy
```

Attached to VLAN:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy2</td>
<td>200-300</td>
</tr>
<tr>
<td>vlan-default</td>
<td>1-199, 301-4094</td>
</tr>
</tbody>
</table>

Attached to ports:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Ports</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy1</td>
<td>Ge1/0/1-4</td>
<td>1-100</td>
</tr>
<tr>
<td>port-default</td>
<td>Ge1/0/1-4</td>
<td>101-4094</td>
</tr>
<tr>
<td></td>
<td>Ge1/0/3-24</td>
<td>1-1094</td>
</tr>
</tbody>
</table>

59.56 show ipv6 first hop security

To display all IPv6 First Hop Security global configuration, use the `show ipv6 first hop security` command in Privilege EXEC configuration mode.

Syntax

`show ipv6 first hop security`

Parameters

N/A

Command Mode

Privilege EXEC configuration mode
User Guidelines

This command displays all IPv6 First Hop Security global configuration.

Example

The following example gives an example of the `show ipv6 first hop security` command:

```
show ipv6 first hop security
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
Logging Packet Drop: enabled
```

59.57  show ipv6 first hop security active policies

To display information about the policies applied to the interface and to the VLAN, use the `show ipv6 first hop security active policies` command in privileged EXEC mode.

Syntax

```
show ipv6 first hop security active policies interface interface-id vlan vlan-id
```

Parameters

- `interface interface-id`—Interface Identifier (Ethernet port or port channel).
- `vlan vlan-id`—VLAN Identifier.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command displays policies applied to frames arriving on given interface and belonging to the given VLAN. The policies are calculated automatically by using the policies attached to the port, VLAN, and the global configuration.
Example
The following example shows the active attached policies on gi1/1/1 and VLAN 100:

```
show ipv6 first hop security active policies interface gi1/1/1 vlan 100
```

IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
IPv6 DHCP Guard is enabled on VLANs:1-4
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
IPv6 Neighbor Binding Integrity is enabled on VLANs:1-4,6,7,100-120
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120

GigaEthernet 1/0/1, VLAN 100
IPv6 First Hop Security Policy:
  - logging packet drop: enabled (from global configuration)
DHCPv6 Guard Policy:
  - device-role: server (from policy1 attached to the interface)
  - reply prefix list name: list10 (from policy2 attached to the VLAN)
  - server address prefix list name: list22 (from policy2 attached to the VLAN)
  - preference
    - minimum: 1 (from policy2 attached to the VLAN)
    - maximum: 200 (from policy2 attached to the VLAN)
ND Inspection Policy:
  - device-role: host (default)
  - drop-unsecure: enabled (from policy2 attached to the VLAN)
  - sec-level minimum: 3 (from policy1 attached to the interface)
  - validate source-mac: enabled (from global configuration)
Neighbor Binding Policy: policy1
  - device-role: perimeter (default)
  - logging binding: enabled (from policy1 attached to the interface)
  - address-prefix-validation: enabled (from policy2 attached to the VLAN)
  - address-prefixes: not defined (default)
  - maximum entries
VLAN: unlimited (from global configuration)
Interface: 1 (from policy1 attached to the interface)
MAC: 2 (from policy2 attached to the VLAN)

RA Guard Policy:
device-role: router (from policy1 attached to the interface)
hop-limit: minimum=10 maximum=200 (from policy2 attached to the VLAN)
manage-config-flag: on (from policy2 attached to the VLAN)
ra address prefix list name: disabled (default)
ra prefixes prefix list name: list1 (from policy2 attached to the VLAN)
other-flag: disabled (default)
router-preference:
  minimum: medium (from policy2 attached to the VLAN)
  maximum: medium (from policy2 attached to the VLAN)

59.58 show ipv6 first hop security attached policies

To display information about the policies attached to the interface and to the VLAN, use the show ipv6 first hop security attached policies command in privileged EXEC mode.

Syntax
show ipv6 first hop security attached policies interface interface-id vlan vlan-id

Parameters
- interface interface-id—Interface Identifier (Ethernet port or port channel).
- vlan vlan-id—VLAN Identifier.

Command Mode
Privilege EXEC configuration mode

User Guidelines
This command displays policies of all IPv6 First Hop Security attached to a VLAN specified by the vlan-id argument and displays all policy attached to a port and to VLAN specified by the interface-id and vlan-id arguments.
Examples

The following example shows the attached policy on gi1/1/1 and VLAN 100:

```
show ipv6 first hop security attached policies interface gi1/1/1 vlan 100
```

Attached to VLAN 100

- RA Guard Policy: policy1
- Neighbor Bind Policy: policy2

Attached to interface gi1/0/1 and VLAN 100

- IPv6 First Hop Security Policy: FHSpolicy
- ND Inspection Policy: policy1
- RA Guard Policy: policy3
- Neighbor Bind Policy: policy3

59.59 show ipv6 first hop security counters

To display information about the packets counted by the interface counter, use the `show ipv6 first hop security counters` command in privileged EXEC mode.

Syntax

```
show ipv6 first hop security counters interface interface-id
```

Parameters

- `interface interface-id`—Displays counters for specified Ethernet port or port channel.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, bridged, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.
**Examples**

**Example 1**—The following examples shows information about packets counted on interface gi1/1:

```
show ipv6 first hop security counters interface gi1/1
```

**Received messages on Gi1/0/1:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Protocol message</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDP</td>
<td>RA[63] RS[0] NA[13] NS[0] REDIR[0]</td>
</tr>
</tbody>
</table>

**Dropped messages on Gi1/0/1:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Protocol message</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDP</td>
<td>RA[2] RS[0] NA[0] NS[0] REDIR[0]</td>
</tr>
</tbody>
</table>

**Dropped reasons on Gi1/0/1:**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Number</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Guard</td>
<td>2</td>
<td>Server msg on client interface</td>
</tr>
<tr>
<td>DHCP Guard</td>
<td>1</td>
<td>Unauthorized assigned address</td>
</tr>
<tr>
<td>DHCP Guard</td>
<td>1</td>
<td>Unauthorized server source address</td>
</tr>
<tr>
<td>DHCP Guard</td>
<td>0</td>
<td>Unauthorized server preference</td>
</tr>
<tr>
<td>RA guard</td>
<td>1</td>
<td>Router msg on host interface</td>
</tr>
<tr>
<td>RA guard</td>
<td>1</td>
<td>Unauthorized source address</td>
</tr>
<tr>
<td>RA guard</td>
<td>0</td>
<td>Unauthorized advertise prefix</td>
</tr>
<tr>
<td>RA guard</td>
<td>0</td>
<td>Unauthorized router preference</td>
</tr>
<tr>
<td>RA guard</td>
<td>0</td>
<td>Unauthorized other config flag</td>
</tr>
<tr>
<td>RA guard</td>
<td>0</td>
<td>Unauthorized managed config flag</td>
</tr>
<tr>
<td>RA guard</td>
<td>0</td>
<td>Unauthorized cur hop limit</td>
</tr>
<tr>
<td>ND Inspection</td>
<td>0</td>
<td>Invalid source MAC</td>
</tr>
<tr>
<td>ND Inspection</td>
<td>0</td>
<td>Unsecure msg</td>
</tr>
<tr>
<td>ND Inspection</td>
<td>0</td>
<td>Unauthorized sec level</td>
</tr>
<tr>
<td>Source guard</td>
<td>0</td>
<td>NoBinding</td>
</tr>
<tr>
<td>NB Integrity</td>
<td>0</td>
<td>Illegal ICMPv6 msg</td>
</tr>
</tbody>
</table>
59.60 show ipv6 nd inspection

To display ND Inspection global configuration, use the `show ipv6 nd inspection` command in Privilege EXEC configuration mode.

**Syntax**

`show ipv6 nd inspection`

**Parameters**

N/A

**Command Mode**

Privilege EXEC configuration mode

**User Guidelines**

This command displays ND Inspection global configuration.

**Example**

The following example gives an example of the `show ipv6 nd snooping` command:

```
show ipv6 nd snooping
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
unsecure drop: enabled
sec-level minimum value: 2
source mac validation: disabled
```

59.61 show ipv6 nd inspection policy

To display an IPv6 ND Inspection policy on all interfaces configured with the ND Inspection feature, use the `show ipv6 nd inspection policy` command in privileged EXEC mode.

**Syntax**

`show ipv6 nd inspection policy [policy-name]`
Parameters

- **policy-name**—Displays the ND Inspection policy with the given name.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command displays the options configured for the ND Inspection policy on all interfaces.

Examples

Example 1—The following example shows the policy configuration for a policy named policy1:

```plaintext
show ipv6 nd inspection policy policy1

ND Inspection Policy: policy1
    device-role: router
    drop-unsecure: enabled
    Attached to VLANs: 1-100,111-4094

Attached to interfaces:
    interface       VLANs
    Ge1/0/5-7       1-58,68-4094
    Ge1/0/8-24,Ge2/0/1-24  1-4094
    Po1-4           1-4094
```

Example 2—The following example shows the attached policies:

```plaintext
show ipv6 nd inspection policy

Attached to VLANs:
    Policy Name | VLANs
    vlan-default | 1-4094

Attached to ports:
    Policy Name | Ports | VLANs
```

IPv6 RA Guard is enabled on VLANs: 1-4, 6, 7, 100-120

"Managed address configuration" flag (M-flag): off

"Other configuration" flag (O-flag): disabled

Hop Limit:
- minimum: 10
- maximum: 100

Default Router Preference:
- minimum: 1
- maximum: 1
59.63 show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the `show ipv6 nd raguard policy` command in privileged EXEC mode.

Syntax

`show ipv6 nd raguard policy [policy-name]`

Parameters

- `policy-name`—Displays the RA guard policy with the given name.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

Example 1—The following example shows the policy configuration for a policy named policy1:

```
show ipv6 nd raguard policy raguard1

RA Guard Policy: policy1
    device-role: router
    router address prefix list name: list1
    prefixes prefix list name: list2
    Attached to VLANs: 1-100,111-4094
    Attached to interfaces:
        interface       VLANs
        Ge1/0/5-7       1-58,68-4094
        Ge1/0/8-24,Ge2/0/1-24  1-4094
        Pol-4           1-4094
```
Example 2—The following example shows the attached policies:

```
show ipv6 nd raguard policy
Attached to VLANs:
    Policy Name  VLANs
    vlan-default  1-4094

Attached to port:
    Policy Name  Ports  VLANs
    port-default  Ge1/0/1-24  1-4094
```

59.64 show ipv6 neighbor binding

To display Neighbor Binding global configuration, use the `show ipv6 neighbor binding` command in Privilege EXEC configuration mode.

Syntax

```
show ipv6 neighbor binding
```

Parameters

N/A

Command Mode

Privilege EXEC configuration mode

User Guidelines

This displays Neighbor Binding global configuration.

Example

The following example gives an example of the `show ipv6 neighbor binding` command:

```
show ipv6 neighbor binding
Neighbor Binding Integrity is enabled on VLANs:1-4,6-7,100-120
Binding logging: disabled
```
59.65 show ipv6 neighbor binding policy

To display Neighbor Binding policies, use the show ipv6 neighbor binding policy command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding policy [policy-name]

Parameters

- **policy-name**—Neighbor Binding policy name.

Command Mode

Privilege EXEC configuration mode

User Guidelines

This displays configured policies or the given one.

Examples

**Example 1**—The following example shows the policy configuration for a policy named policy1:

```plaintext
show ipv6 neighbor binding policy policy1
```

Neighbor Binding Policy: policy1

- device-role: perimeter
- binding logging: disabled
- max-entries
- VLAN: unlimited
- Interface: 10
MAC: 2
Attached to VLANs: 1-100, 111-4094

Attached to ports:

<table>
<thead>
<tr>
<th>interface</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ge1/0/5-7</td>
<td>1-58, 68-4094</td>
</tr>
<tr>
<td>Ge1/0/8-24, Ge2/0/1-24</td>
<td>1-4094</td>
</tr>
<tr>
<td>Po1-4</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Example 2—The following example shows the attached policies:

show ipv6 neighbor binding policy

Attached to VLAN:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy2</td>
<td>200-300</td>
</tr>
<tr>
<td>vlan-default</td>
<td>1-199, 301-4094</td>
</tr>
</tbody>
</table>

Attached to ports:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Ports</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy1</td>
<td>Ge1/0/1-4</td>
<td>1-100</td>
</tr>
<tr>
<td>port-default</td>
<td>Ge1/0/1-4</td>
<td>101-4094</td>
</tr>
</tbody>
</table>

59.66 show ipv6 neighbor binding table

To display contents of the Binding table, use the show ipv6 neighbor binding table command in Privilege EXEC configuration mode.

Syntax

```
show ipv6 neighbor binding table [vlan vlan-id] [interface interface-id] [ipv6 ipv6-address] [mac mac-address]
```

Parameters

- `vlan vlan-id`—Displays the Binding table entries that match the specified VLAN.
• **interface interface-id**—Displays the Binding table entries that match the specified interface (Ethernet port or port channel).

• **ipv6 ipv6-address**—Displays the Binding table entries that match the specified IPv6 address.

• **mac mac-address**—Displays the Binding table entries that match the specified MAC address.

**Command Mode**

Privilege EXEC configuration mode

**User Guidelines**

This displays the contents of the Binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all Binding table contents are displayed.

Any keyword and argument combinations are allowed.

**Example**

The following example displays the contents of the Binding table:

```
show ipv6 neighbor binding table
```

Binding Table has 3 entries

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IPv6 address</th>
<th>Inter</th>
<th>MAC address</th>
<th>Origin</th>
<th>State</th>
<th>Expir Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2001:300::1</td>
<td>gi1/1/1</td>
<td>AABB.CC01.F500</td>
<td>NDP</td>
<td>VALID</td>
<td>559</td>
</tr>
<tr>
<td>100</td>
<td>2001:600::1</td>
<td>gi1/1/1</td>
<td>AABB.CC01.F500</td>
<td>NDP</td>
<td>TENT</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>2001:100::2</td>
<td>gi1/1/2</td>
<td>AABB.CC01.F600</td>
<td>NDP</td>
<td>VALID</td>
<td>96</td>
</tr>
</tbody>
</table>

**Field Descriptions:**

- **VLAN**—VLAN the host belongs to.

- **IPv6 address**—IPv6 address of the host.

- **Inter**—Interface the host is connected on.

- **MAC address**—MAC address of the host.
### Origin
- **Static**—The static IPv6 address manually defined by the `ipv6 neighbor binding static` command.
- **NDP**—The IPv6 address learnt from the NDP protocol messages.
- **DHCP**—The IPv6 address learnt from the DHCPv6 protocol messages.

### State
- **TENT**—The new host IPv6 address is under validation. Since its lifetime is less than 1sec its expiration time is not displayed.
- **VALID**—The host IPv6 address was bound.
- **Expir. Time**—Left time in seconds until the entry will be removed, if it is not confirmed.

---

### 59.67 validate source-mac

To enable checking the MAC addresses against the link-layer address within an IPv6 ND Inspection policy, use the `validate source-mac` command in ND Inspection Policy Configuration mode. To return to the default, use the `no` form of this command.

**Syntax**

```
validate source-mac [enable | disable]
```

**Parameters**

- **enable**—Enables validation of the MAC address against the link-layer address. If no keyword is configured, the keyword is applied by default.
- **disable**—Disables validation of MAC address against the link-layer address.

**Default Configuration**

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.
Command Mode

ND inspection Policy Configuration (config-nd-inspection)

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables the router to drop an NDP message whose link-layer address does not match the MAC address:

```
ipv6 nd inspection policy policy1
    validate source-mac

exit
```